FortiOS™ Handbook - Authentication

VERSION 5.2.6

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

March 9, 2016

FortiOS™ Handbook - Authentication

01-526-122870-20160309

TABLE OF CONTENTS

Change log

Date	Change Description
2016-03-09	Added information re: LDAP user group support in PAP/CHAP protocols. Minor other updates.
2015-12-18	Improved Examples and Troubleshooting on page 180
2015-12-17	Improved Monitoring authenticated users on page 177
2015-12-14	Improved SSO using RADIUS accounting records on page 170
2015-11-09	Improved Agent-based FSSO on page 126
2015-10-29	Improved Single Sign-On to Windows AD on page 118
2015-10-22	Improved Single Sign-On using a FortiAuthenticator unit on page 114
2015-10-14	Improved Certificate-based authentication on page 95
2015-10-09	Improved Captive portals on page 87
2015-10-02	Improved Configuring authenticated access on page 71
2015-09-25	Improved Managing Guest Access on page 66
2015-06-20	Improved Users and user groups on page 46
2015-05-22	Improved Authentication servers on page 22
2015-04-14	Updated Introduction to authentication on page 13
2015-03-31	Initial release.

Introduction

Welcome and thank you for selecting Fortinet products for your network protection.

This chapter contains the following topics:

Before you begin

Before you begin using this guide, please ensure that:

- You have administrative access to the web-based manager and/or CLI.
- The FortiGate unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.
- Any third-party software or servers have been configured using their documentation.

While using the instructions in this guide, note that administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

How this guide is organized

This Handbook chapter contains the following sections:

Introduction to authentication describes some basic elements and concepts of authentication.

Authentication servers describes external authentication servers, where a FortiGate unit fits into the topology, and how to configure a FortiGate unit to work with that type of authentication server.

Users and user groups describes the different types of user accounts and user groups. Authenticated access to resources is based on user identities and user group membership. Two-factor authentication methods, including FortiToken, provide additional security.

Managing Guest Access explains how to manage temporary accounts for visitors to your premises.

Configuring authenticated access provides detailed procedures for setting up authenticated access in security policies and authenticated access to VPNs.

Captive portals describes how to authenticate users through a web page that the FortiGate unit presents in response to any HTTP request until valid credentials are entered. This can be used for wired or WiFi network interfaces.

Certificate-based authentication describes authentication by means of X.509 certificates.

Single Sign-On using a FortiAuthenticator unit describes how to use a FortiAuthenticator unit as an SSO agent that can integrate with external network authentication systems such as RADIUS and LDAP to gather user logon information and send it to the FortiGate unit. Users can also log on through a FortiAuthenticator-based web portal or the FortiClient SSO Mobility Agent.

Single Sign-On to Windows AD describes how to set up Single Sign-On in a Windows AD network by configuring the FortiGate unit to poll domain controllers for information user logons and user privileges.

Agent-based FSSO describes how to set up Single Sign-On in Windows AD, Citrix, or Novell networks by installing Fortinet Single Sign On (FSSO) agents on domain controllers. The FortiGate unit receives information about user logons and allows access to network resources based on user group memberships.

SSO using RADIUS accounting records describes how to set up Single Sign-On in a network that uses RADIUS authentication. In this configuration, the RADIUS server send RADIUS accounting records to the FortiGate unit when users log on or off the network. The record includes a user group name that can be used in FortiGate security policies to determine which resources each user can access.

Monitoring authenticated users describes FortiOS authenticated user monitor screens.

Examples and Troubleshooting provides configuration examples and troubleshooting suggestions.

Introduction to authentication

Identifying users and other computers—authentication—is a key part of network security. This section describes some basic elements and concepts of authentication.

The following topics are included in this section:

What is authentication?

Businesses need to authenticate people who have access to company resources. In the physical world this may be a swipe card to enter the building, or a code to enter a locked door. If a person has this swipe card or code, they have been authenticated as someone allowed in that building or room.

Authentication is the act of confirming the identity of a person or other entity. In the context of a private computer network, the identities of users or host computers must be established to ensure that only authorized parties can access the network. The FortiGate unit enables controlled network access and applies authentication to users of security policies and VPN clients.

Methods of authentication

FortiGate unit authentication is divided into three basic types: password authentication for people, certificate authentication for hosts or endpoints, and two-factor authentication for additional security beyond just passwords. An exception to this is that FortiGate units in an HA cluster and FortiManager units use password authentication.

Password authentication verifies individual user identities, but access to network resources is based on membership in user groups. For example, a security policy can be configured to permit access only to the members of one or more user groups. Any user who attempts to access the network through that policy is then authenticated through a request for their username and password.

Methods of authentication include:

Local password authentication

The simplest authentication is based on user accounts stored locally on the FortiGate unit. For each account, a username and password is stored. The account also has a disable option so that you can suspend the account without deleting it.

Local user accounts work well for a single-FortiGate installation. If your network has multiple FortiGate units that will use the same accounts, the use of an external authentication server can simplify account configuration and maintenance.

You can create local user accounts in the web-based manager under **User & Device > User > User Definition**. This page is also used to create accounts where an external authentication server stores and verifies the password.

Server-based password authentication

Using external authentication servers is desirable when multiple FortiGate units need to authenticate the same users, or where the FortiGate unit is added to a network that already contains an authentication server. FortiOS supports the use of LDAP, RADIUS, TACACS+, AD or POP3 servers for authentication.

When you use an external authentication server to authenticate users, the FortiGate unit sends the user's entered credentials to the external server. The password is encrypted. The server's response indicates whether the supplied credentials are valid or not.

You must configure the FortiGate unit to access the external authentication servers that you want to use. The configuration includes the parameters that authenticate the FortiGate unit to the authentication server.

You can use external authentication servers in two ways:

- Create user accounts on the FortiGate unit, but instead of storing each user's password, specify the server used to authenticate that user. As with accounts that store the password locally, you add these users to appropriate user groups.
- Add the authentication server to user groups. Any user who has an account on the server can be authenticated and have the access privileges of the FortiGate user group. Optionally, when an LDAP server is a FortiGate user group member, you can limit access to users who belong to specific groups defined on the LDAP server.

Certificate-based authentication

An RSA X.509 server certificate is a small file issued by a Certificate Authority (CA) that is installed on a computer or FortiGate unit to authenticate itself to other devices on the network. When one party on a network presents the certificate as authentication, the other party can validate that the certificate was issued by the CA. The identification is therefore as trustworthy as the Certificate Authority (CA) that issued the certificate.

To protect against compromised or misused certificates, CAs can revoke any certificate by adding it to a Certificate Revocation List (CRL). Certificate status can also be checked online using Online Certificate Status Protocol (OCSP).

RSA X.509 certificates are based on public-key cryptography, in which there are two keys: the private key and the public key. Data encrypted with the private key can be decrypted only with the public key and vice versa. As the names suggest, the private key is never revealed to anyone and the public key can be freely distributed. Encryption with the recipient's public key creates a message that only the intended recipient can read. Encryption

with the sender's private key creates a message whose authenticity is proven because it can be decrypted only with the sender's public key.

Server certificates contain a signature string encrypted with the CA's private key. The CA's public key is contained in a CA root certificate. If the signature string can be decrypted with the CA's public key, the certificate is genuine.

Certificate authorities

A certificate authority can be:

- an organization, such as VeriSign Inc., that provides certificate services
- a software application, such as Microsoft Certificate Services or OpenSSH

For a company web portal or customer-facing SSL VPN, a third-party certificate service has some advantages. The CA certificates are already included in popular web browsers and customers trust the third-party. On the other hand, third-party services have a cost.

For administrators and for employee VPN users, the local CA based on a software application provides the required security at low cost. You can generate and distribute certificates as needed. If an employee leaves the organization, you can simply revoke their certificate.

Certificates for users

FortiGate unit administrators and SSL VPN users can install certificates in their web browsers to authenticate themselves. If the FortiGate unit uses a CA-issued certificate to authenticate itself to the clients, the browser will also need the appropriate CA certificate.

FortiGate IPsec VPN users can install server and CA certificates according to the instructions for their IPsec VPN client software. The FortiClient Endpoint Security application, for example, can import and store the certificates required by VPN connections.

FortiGate units are also compatible with some Public Key Infrastructure systems. For an example of this type of system, see RSA ACE (SecurID) servers on page 40.

Two-factor authentication

A user can be required to provide both something they know (their username and password combination) and something they have (certificate or a random token code). Certificates are installed on the user's computer.

Two-factor authentication is available for PKI users. For more information, see Certificate on page 51.

Another type of two-factor authentication is to use a randomly generated token (multi-digit number) along with the username and password combination. One method is a FortiToken — a one time passcode (OTP) generator that generates a unique code every 60 seconds. Others use email or SMS text messaging to deliver the random token code to the user or administrator.

When one of these methods is configured, the user enters this code at login after the username and password have been verified. The FortiGate unit verifies the token code after as well as the password and username. For more information, see Two-factor authentication on page 50

Types of authentication

FortiOS supports two different types of authentication based on your situation and needs.

Security policy authentication is easily applied to all users logging on to a network, or network service. For example if a group of users on your network such as the accounting department who have access to sensitive data need to access the Internet, it is a good idea to make sure the user is a valid user and not someone trying to send company secrets to the Internet. Security policy authentication can be applied to as many or as few users as needed, and it supports a number of authentication protocols to easily fit with your existing network.

Virtual Private Network (VPN) authentication enables secure communication with hosts located outside the company network, making them part of the company network while the VPN tunnel is operating. Authentication applies to the devices at both ends of the VPN and optionally VPN users can be authenticated as well.

Security policy authentication

Security policies enable traffic to flow between networks. Optionally, the policy can allow access only to specific originating addresses, device types, users or user groups. Where access is controlled by user or user group, users must authenticate by entering valid username and password credentials.

The user's authentication expires if the connection is idle for too long, 5 minutes by default but that can be customized.

Security policies are the mechanism for FSSO, NTLM, certificate based, and RADIUS SSO authentication.

FSSO

Fortinet Single Sign on (FSSO) provides seamless authentication support for Microsoft Windows Active Directory (AD) and Novell eDirectory users in a FortiGate environment.

On a Microsoft Windows or Novell network, users authenticate with the Active Directory or Novell eDirectory at logon. FSSO provides authentication information to the FortiGate unit so that users automatically get access to permitted resources. See Introduction to agent-based FSSO on page 126.

NTLM

The NT LAN Manager (NTLM) protocol is used when the MS Windows Active Directory (AD) domain controller can not be contacted. NTLM is a browser-based method of authentication.

The FSSO software is installed on each AD server and the FortiGate unit is configured to communicate with each FSSO client. When a user successfully logs into their Windows PC (and is authenticated by the AD Server), the FSSO client communicates the user's name, IP address, and group login information to the FortiGate unit. The FortiGate unit sets up a temporary access policy for the user, so when they attempt access through the firewall they do not need to re-authenticate. This model works well in environments where the FSSO client can be installed on all AD servers.

In system configurations where it is not possible to install FSSO clients on all AD servers, the FortiGate unit must be able to query the AD servers to find out if a user has been properly authenticated. This is achieved using the NTLM messaging features of Active Directory and Internet Explorer.

Even when NTLM authentication is used, the user is not asked again for their username and password. Internet Explorer stores the user's credentials and the FortiGate unit uses NTLM messaging to validate them in the Windows AD environment.

Note that if the authentication reaches the timeout period, the NTLM message exchange restarts. For more information on NTLM, see NTLM authentication on page 80 and FSSO NTLM authentication support on page 132.

Certificates

Certificates can be used as part of a policy. All users being authenticated against the policy are required to have the proper certificate. See Certificate-based authentication on page 95

RADIUS SSO

RADIUS Single Sign-On (RSSO) is a remote authentication method that does not require any local users to be configured, and relies on RADIUS Start records to provide the FortiGate unit with authentication information. That information identifies the user and user group, which is then matched using a security policy. See SSO using RADIUS accounting records on page 170.

FortiGuard Web Filter override authentication

Optionally, users can be allowed the privilege of overriding FortiGuard Web Filtering to view blocked web sites. Depending on the override settings, the override can apply to the user who requested it, the entire user group to which the user belongs, or all users who share the same web filter profile. As with other FortiGate features, access to FortiGuard overrides is controlled through user groups. Firewall and Directory Services user groups are eligible for the override privilege. For more information about web filtering and overrides, see the UTM chapter of this FortiOS Handbook.

VPN authentication

Authentication involves authenticating the user. In IPsec VPNs authenticating the user is optional, but authentication of the peer device is required.

This section includes:

- Authenticating IPsec VPN peers (devices)
- Authenticating IPsec VPN users
- Authenticating SSL VPN users
- Authenticating PPTP and L2TP VPN users

Authenticating IPsec VPN peers (devices)

A VPN tunnel has one end on a local trusted network, and the other end is at a remote location. The remote peer (device) must be authenticated to be able to trust the VPN tunnel. Without that authentication, it is possible for a malicious hacker to masquerade as a valid VPN tunnel device and gain access to the trusted local network.

The three ways to authenticate VPN peers are with a preshared key, RSA X.509 certificate, or a specific peer ID value.

The simplest way for IPsec VPN peers to authenticate each other is through the use of a preshared key, also called a shared secret. The preshared key is a text string used to encrypt the data exchanges that establish the VPN tunnel. The preshared key must be six or more characters. The VPN tunnel cannot be established if the two peers do not use the same key. The disadvantage of preshared key authentication is that it can be difficult to securely distribute and update the preshared keys.

RSA X.509 certificates are a better way for VPN peers to authenticate each other. Each peer offers a certificate signed by a Certificate Authority (CA) which the other peer can validate with the appropriate CA root certificate. For more information about certificates, see Certificate-based authentication on page 95.

You can supplement either preshared key or certificate authentication by requiring the other peer to provide a specific peer ID value. The peer ID is a text string configured on the peer device. On a FortiGate peer or FortiClient Endpoint Security peer, the peer ID provided to the remote peer is called the Local ID.

Authenticating IPsec VPN users

An IPsec VPN can be configured to accept connections from multiple dynamically addressed peers. You would do this to enable employees to connect to the corporate network while traveling or from home. On a FortiGate unit, you create this configuration by setting the **Remote Gateway** to **Dialup User**.

It is possible to have an IPsec VPN in which remote peer devices authenticate using a common preshared key or a certificate, but there is no attempt to identify the user at the remote peer. To add user authentication, you can do one of the following:

- require a unique preshared key for each peer
- require a unique peer ID for each peer
- require a unique peer certificate for each peer
- require additional user authentication (XAuth)

The peer ID is a text string configured on the peer device. On a FortiGate peer or FortiClient Endpoint Security peer, the peer ID provided to the remote peer is called the Local ID.

Authenticating SSL VPN users

SSL VPN users can be

- user accounts with passwords stored on the FortiGate unit
- user accounts authenticated by an external RADIUS, LDAP or TACACS+ server
- PKI users authenticated by certificate

You need to create a user group for your SSL VPN. Simply create a firewall user group, enable SSL VPN access for the group, and select the web portal the users will access.

SSL VPN access requires an SSL VPN security policy that permits access to members of your user group.

Authenticating PPTP and L2TP VPN users

PPTP and L2TP are older VPN tunneling protocols that do not provide authentication themselves. FortiGate units restrict PPTP and L2TP access to users who belong to one specified user group. Users authenticate themselves to the FortiGate unit by username/password. You can configure PPTP and L2TP VPNs only in the CLI. Before you configure the VPN, create a firewall user group and add to it the users who are permitted to use the VPN. Users are authenticated when they attempt to connect to the VPN. For more information about configuring PPTP or L2TP VPNs, see the FortiGate CLI Reference.

Single Sign-On authentication for users

“Single Sign-On” means that users logged on to a computer network are authenticated for access to network resources through the FortiGate unit without having to enter their username and password again. FortiGate units directly provide Single Sign On capability for:

- Microsoft Windows networks using either Active Directory or NTLM authentication
- Novell networks, using eDirectory

In combination with a FortiAuthenticator unit, the FortiGate unit can provide Single Sign-On capability that integrates multiple external network authentication systems such as Windows Active Directory, Novell e-Directory, RADIUS and LDAP. The FortiAuthenticator unit gathers user logon information from all of these sources and sends it to the FortiGate unit.

Through the SSO feature, the FortiGate unit knows the username, IP address, and external user groups to which the user belongs. When the user tries to access network resources, the FortiGate unit selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

For detailed information about SSO, see

- Single Sign-On using a FortiAuthenticator unit on page 114
- Agent-based FSSO on page 126

User's view of authentication

From the user's point of view, they see a request for authentication when they try to access a protected resource, such as an FTP repository of intellectual property or simply access a website on the Internet. The way the request is presented to the user depends on the method of access to that resource.

VPN authentication usually controls remote access to a private network.

Web-based user authentication

Security policies usually control browsing access to an external network that provides connection to the Internet. In this case, the FortiGate unit requests authentication through the web browser.

The user types a username and password and then selects **Continue** or **Login**. If the credentials are incorrect, the authentication screen is redisplayed with blank fields so that the user can try again. When the user enters valid credentials, access is granted to the required resource. In some cases, if a user tries to authenticate several times without success, a message appears, such as: "Too many bad login attempts. Please try again in a few minutes." This indicates the user is locked out for a period of time. This prevents automated brute force password hacking attempts. The administrator can customize these settings if required.

After a defined period of user inactivity (the authentication timeout, defined by the FortiGate administrator), the user's access expires. The default is 5 minutes. To access the resource, the user will have to authenticate again.

VPN client-based authentication

A VPN provides remote clients with access to a private network for a variety of services that include web browsing, email, and file sharing. A client program such as FortiClient negotiates the connection to the VPN and manages the user authentication challenge from the FortiGate unit.

FortiClient can store the username and password for a VPN as part of the configuration for the VPN connection and pass them to the FortiGate unit as needed. Or, FortiClient can request the username and password from the user when the FortiGate unit requests them.

SSL VPN is a form of VPN that can be used with a standard Web browser. There are two modes of SSL VPN operation (supported in NAT/Route mode only):

- web-only mode, for remote clients equipped with a web-browser only
- tunnel mode, for remote computers that run a variety of client and server applications.

After a defined period of user inactivity on the VPN connection (the idle timeout, defined by the FortiGate administrator), the user's access expires. The default is 30 minutes. To access the resource, the user will have to authenticate again.

FortiGate administrator's view of authentication

Authentication is based on user groups. The FortiGate administrator configures authentication for security policies and VPN tunnels by specifying the user groups whose members can use the resource. Some planning is required to determine how many different user groups need to be created. Individual user accounts can belong to multiple groups, making allocation of user privileges very flexible.

A member of a user group can be:

- a user whose username and password are stored on the FortiGate unit
- a user whose name is stored on the FortiGate unit and whose password is stored on a remote or external authentication server
- a remote or external authentication server with a database that contains the username and password of each person who is permitted access

The general process of setting up authentication is as follows:

1. If remote or external authentication is needed, configure the required servers.
2. Configure local and peer (PKI) user identities. For each local user, you can choose whether the FortiGate unit or a remote authentication server verifies the password. Peer members can be included in user groups for use in security policies.
3. Create user groups.
4. Add local/peer user members to each user group as appropriate. You can also add an authentication server to a user group. In this case, all users in the server's database can authenticate. You can only configure peer user groups through the CLI.
5. Configure security policies and VPN tunnels that require authenticated access.

For authentication troubleshooting, see the specific chapter for the topic or for general issues see Troubleshooting on page 196.

General authentication settings

Go to **User & Device > Authentication > Settings** to configure authentication timeout, protocol support, and authentication certificates.

When user authentication is enabled within a security policy, the authentication challenge is normally issued for any of the four protocols (depending on the connection protocol):

- HTTP (can also be set to redirect to HTTPS)
- HTTPS
- FTP
- Telnet

The selections made in the **Protocol Support** list of **Authentication Settings** control which protocols support the authentication challenge. Users must connect with a supported protocol first so they can subsequently connect with other protocols. If HTTPS is selected as a method of protocol support, it allows the user to authenticate with a customized Local certificate.

When you enable user authentication within a security policy, the security policy user will be challenged to authenticate. For user ID and password authentication, users must provide their user names and passwords. For certificate authentication (HTTPS or HTTP redirected to HTTPS only), you can install customized certificates on the unit and the users can also have customized certificates installed on their browsers. Otherwise, users will see a warning message and have to accept a default Fortinet certificate.

Authentication Timeout	Enter a length of time in minutes, from 1 to 1440 (24 hours). Authentication timeout controls how long an authenticated firewall connection can be idle before the user must authenticate again. The default value is 5.
Protocol Support	Select the protocols to challenge during firewall user authentication.
Certificate	If using HTTPS protocol support, select the local certificate to use for authentication. Available only if HTTPS protocol support is selected.
Apply	Select to apply the selections for user authentication settings.

Authentication servers

FortiGate units support the use of external authentication servers. An authentication server can provide password checking for selected FortiGate users or it can be added as a member of a FortiGate user group.

If you are going to use authentication servers, you must configure the servers before you configure FortiGate users or user groups that require them.

Mac OS and iOS devices, including iPhones and iPads, can perform user authentication with FortiOS units using RADIUS servers, but not with LDAP or TACACS+ servers.

This section includes the following topics:

FortiAuthenticator servers

FortiAuthenticator is an Authentication, Authorization, and Accounting (AAA) server, that includes a RADIUS server, an LDAP server, and can replace the FSSO Collector Agent on a Windows AD network. Multiple FortiGate units can use a single FortiAuthenticator for FSSO, remote authentication, and FortiToken management.

For more information, see the FortiAuthenticator Administration Guide.

RADIUS servers

Remote Authentication and Dial-in User Service (RADIUS) is a broadly supported client-server protocol that provides centralized authentication, authorization, and accounting functions. RADIUS clients are built into gateways that allow access to networks such as Virtual Private Network servers, Network Access Servers (NAS), as well as network switches and firewalls that use authentication. FortiGate units fall into the last category.

RADIUS servers use UDP packets to communicate with the RADIUS clients on the network to authenticate users before allowing them access to the network, to authorize access to resources by appropriate users, and to account or bill for those resources that are used. RADIUS servers are currently defined by RFC 2865 (RADIUS) and RFC 2866 (Accounting), and listen on either UDP ports 1812 (authentication) and 1813 (accounting) or ports 1645 (authentication) and 1646 (accounting) requests. RADIUS servers exist for all major operating systems.

You must configure the RADIUS server to accept the FortiGate unit as a client. FortiGate units use the authentication and accounting functions of the RADIUS server.

FortiOS does not accept all characters from auto generated keys from MS Windows 2008. These keys are very long and as a result RADIUS authentication will not work. Maximum key length for MS Windows 2008 is 128 bytes. In older versions of FSAE, it was 40 bytes.

Microsoft RADIUS servers

Microsoft Windows Server 2000, 2003, and 2008 have RADIUS support built-in. Microsoft specific RADIUS features are defined in RFC 2548. The Microsoft RADIUS implementation can use Active Directory for user credentials.

For details on Microsoft RADIUS server configurations, refer to Microsoft documentation.

RADIUS user database

The RADIUS user database is commonly an SQL or LDAP database, but can also be any combination of:

- usernames and passwords defined in a configuration file
- user account names and passwords configured on the computer where the RADIUS server is installed.

If users are members of multiple RADIUS groups, then the user group authentication timeout value does not apply. See Membership in multiple groups on page 62.

RADIUS authentication with a FortiGate unit

To use RADIUS authentication with a FortiGate unit

- configure one or more RADIUS servers on the FortiGate unit
- assign users to a RADIUS server

When a configured user attempts to access the network, the FortiGate unit will forward the authentication request to the RADIUS server which will match the username and password remotely. Once authenticated the RADIUS server passes the authorization granted message to the FortiGate unit which grants the user permission to access the network.

The RADIUS server uses a “shared secret” key along with MD5 hashing to encrypt information passed between RADIUS servers and clients, including the FortiGate unit. Typically only user credentials are encrypted. Additional security can be configured through IPsec tunnels.

RADIUS attribute value pairs

RADIUS packets include a set of attribute value pairs (AVP) to identify information about the user, their location and other information. The FortiGate unit sends the following RADIUS attributes.

FortiOS supported RADIUS attributes

RADIUS Attribute	Name	Description	AVP type
1	Acct-Session-ID	Unique number assigned to each start and stop record to make it easy to match them, and to eliminate duplicate records.	44
2	username	Name of the user being authenticated	1
3	NAS-Identifier	Identifier or IP address of the Network Access Server (NAS) that is requesting authentication. In this case, the NAS is the FortiGate unit.	32
4	Framed-IP-Address	Address to be configured for the user.	8
5	Fortinet-VSA	See Vendor-specific attributes on page 25	26
6	Acct-Input-Octets	Number of octets received from the port over the course of this service being provided. Used to charge the user for the amount of traffic they used.	42
7	Acct-Output-Octets	Number of octets sent to the port while delivering this service. Used to charge the user for the amount of traffic they used.	43

The following table describes the supported authentication events and the RADIUS attributes that are sent in the RADIUS accounting message.

RADIUS attributes sent in RADIUS accounting message

	RADIUS Attributes						
Authentication Method	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Web	X	X	X		X		
XAuth of IPsec (without DHCP)	X	X	X		X		
XAuth of IPsec (with DHCP)	X	X	X	X	X		
PPTP/L2TP (in PPP)	X	X	X	X	X	X	X
SSL-VPN	X	X	X		X		

Vendor-specific attributes

Vendor specific attributes (VSA) are the method RADIUS servers and client companies use to extend the basic functionality of RADIUS. Some major vendors, such as Microsoft, have published their VSAs, however many do not.

In order to support vendor-specific attributes (VSA), the RADIUS server requires a dictionary to define which VSAs to support. This dictionary is typically supplied by the client or server vendor.

The Fortinet RADIUS vendor ID is 12356.

The FortiGate unit RADIUS VSA dictionary is supplied by Fortinet and is available through the Fortinet Knowledge Base (http://kb.forticare.com) or through Technical Support. Fortinet's dictionary for FortiOS 4.0 and up is configured this way:

```
##
Fortinet's VSA's
#
VENDOR fortinet 12356
BEGIN-VENDOR fortinet
ATTRIBUTE Fortinet-Group-Name   1   string
ATTRIBUTE Fortinet-Client-IP-Address   2   ipaddr
ATTRIBUTE Fortinet-Vdom-Name   3   string
ATTRIBUTE Fortinet-Client-IPv6-Address   4   octets
ATTRIBUTE Fortinet-Interface-Name   5   string
ATTRIBUTE Fortinet-Access-Profile   6   string
#
# Integer Translations
#
END-VENDOR Fortinet
```

Note that using the Fortinet-Vdom-Name, users can be tied to a specific VDOM on the FortiGate unit. See the documentation provided with your RADIUS server for configuration details.

Role Based Access Control

In Role Based Access Control (RBAC), network administrators and users have varying levels of access to network resources based on their role, and that role's requirement for access specific resources. For example, a junior accountant does not require access to the sales presentations, or network user account information.

There are three main parts to RBAC: role assignment, role authorization, and transaction authorization. Role assignment is accomplished when someone in an organization is assigned a specific role by a manager or HR. Role authorization is accomplished when a network administrator creates that user's RADIUS account and assigns them to the required groups for that role. Transaction authorization occurs when that user logs on and authenticates before performing a task.

RBAC is enforced when FortiOS network users are remotely authenticated via a RADIUS server. For users to authenticate, a security policy must be matched. That policy only matches a specific group of users. If VDOMs are enabled, the matched group will be limited to a specific VDOM. Using this method network administrators can separate users into groups that match resources, protocols, or VDOMs. It is even possible to limit users to specific FortiGate units if the RADIUS servers serve multiple FortiOS units.

For more information on security policies, see Authentication in security policies on page 75.

Configuring the FortiGate unit to use a RADIUS server

The information you need to configure the FortiGate unit to use a RADIUS server includes

- the RADIUS server's domain name or IP address
- the RADIUS server's shared secret key.

You can optionally specify the NAS IP or Called Station ID. When configuring the FortiGate to use a RADIUS server, the FortiGate is a Network Access Server (NAS). If the FortiGate interface has multiple IP addresses, or you want the RADIUS requests to come from a different address you can specify it here. Called Station ID applies to carrier networks. However, if the NAS IP is not included in the RADIUS configuration, the IP of the FortiGate unit interface that communicates with the RADIUS server is used instead.

A maximum of 10 remote RADIUS servers can be configured on the FortiGate unit. One or more servers must be configured on FortiGate before remote users can be configured. To configure remote users, see Local and remote users on page 47.

On the FortiGate unit, the default port for RADIUS traffic is 1812. Some RADIUS servers use port 1645. If this is the case with your server, you can either:

- Re-configure the RADIUS server to use port 1812. See your RADIUS server documentation for more information on this procedure.

or

- Change the FortiGate unit default RADIUS port to 1645 using the CLI:

```
config system global
   set radius-port 1645
end
```

One wildcard admin account can be added to the FortiGate unit when using RADIUS authentication. This uses the wildcard character to allow multiple admin accounts on RADIUS to use a single account on the FortiGate unit. See Example — wildcard admin accounts - CLI on page 33.

To configure the FortiGate unit for RADIUS authentication - web-based manager:

1. Go to **User & Device > Authentication > RADIUS Servers** and select **Create New**.
2. Enter the following information and select **OK**.

Name	A name to identify the RADIUS server on the FortiGate unit.
Primary Server Name/IP	Enter the domain name (such as fgt.exmaple.com) or the IP address of the RADIUS server.
Primary Server Secret	Enter the server secret key, such as radiusSecret. This can be a maximum of 16 characters long. This must match the secret on the RADIUS primary server.
Secondary Server Name/IP	Optionally enter the domain name (such as fgt.exmaple.com) or the IP address of the secondary RADIUS server.

Secondary Server Secret	Optionally, enter the secondary server secret key, such as radiusSecret2. This can be a maximum of 16 characters long. This must match the secret on the RADIUS secondary server.
Authentication Scheme	If you know the RADIUS server uses a specific authentication protocol, select it from the list. Otherwise select **Use Default Authentication Scheme**. The Default option will usually work.
NAS IP/ Called Station ID	Enter the IP address to be used as an attribute in RADIUS access requests. **NAS-IP-Address** is RADIUS setting or IP address of FortiGate interface used to talk to RADIUS server, if not configured. **Called Station ID** is same value as NAS-IP Address but in text format.
Include in every User Group	When enabled this RADIUS server will automatically be included in all user groups. This is useful if all users will be authenticating with the remote RADIUS server.

For MAC OS and iOS devices to authenticate, you must use MS-CHAP-v2 authentication. In the CLI, the command is `set auth-type ms_chap_v2`.

3. Select **OK**.

To configure the FortiGate unit for RADIUS authentication - CLI example:

```
config user radius
   edit ourRADIUS
      set auth-type auto
      set server 10.11.102.100
      set secret radiusSecret
   end
```

For more information about RADIUS server options, refer to the FortiGate CLI Reference.

Troubleshooting RADIUS

To test the connection to the RADIUS server use the following command:

```
diagnose test authserver radius-direct <server_name or IP> <port number> <secret>
```

For the port number, enter `-1` to use the default port. Otherwise enter the port number to check.

LDAP servers

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of

a data-representation scheme, a set of defined operations, and a request/response network.

The scale of LDAP servers range from big public servers such as BigFoot and Infospace, to large organizational servers at universities and corporations, to small LDAP servers for workgroups that may be using OpenLDAP. This document focuses on the institutional and workgroup applications of LDAP.

This section includes:

Components and topology

LDAP organization starts with directories. A directory is a set of objects with similar attributes organized in a logical and hierarchical way. Generally, an LDAP directory tree reflects geographic and organizational boundaries, with the Domain name system (DNS) names to structure the top level of the hierarchy. The common name identifier for most LDAP servers is `cn`, however some servers use other common name identifiers such as `uid`.

When LDAP is configured and a user is required to authenticate the general steps are:

1. The FortiGate unit contacts the LDAP server for authentication.
2. To authenticate with the FortiGate unit, the user enters a username and password.
3. The FortiGate unit sends this username and password to the LDAP server.
4. If the LDAP server can authenticate the user, the user is successfully authenticated with the FortiGate unit.
5. If the LDAP server cannot authenticate the user, the connection is refused by the FortiGate unit.

Binding

Binding is the step where the LDAP server authenticates the user. If the user is successfully authenticated, binding allows the user access to the LDAP server based on that user's permissions.

The FortiGate unit can be configured to use one of three types of binding:

- anonymous - bind using anonymous user search
- regular - bind using username/password and then search
- simple - bind using a simple password authentication without a search

You can use simple authentication if the user records all fall under one domain name (`dn`). If the users are under more than one `dn`, use the anonymous or regular type, which can search the entire LDAP database for the required username.

If your LDAP server requires authentication to perform searches, use the regular type and provide values for username and password.

Supported versions

The FortiGate unit supports LDAP protocol functionality defined in RFC 2251: Lightweight Directory Access Protocol v3, for looking up and validating user names and passwords. FortiGate LDAP supports all LDAP servers

compliant with LDAP v3, including FortiAuthenticator. In addition, FortiGate LDAP supports LDAP over SSL/TLS, which can be configured only in the CLI.

FortiGate LDAP does not support proprietary functionality, such as notification of password expiration, which is available from some LDAP servers. FortiGate LDAP does not supply information to the user about why authentication failed.

LDAP user authentication is supported for PPTP, L2TP, IPsec VPN, and firewall authentication.

However, with PPTP, L2TP, and IPsec VPN, PAP (Packet Authentication Protocol) is supported, while CHAP (Challenge Handshake Authentication Protocol) is not.

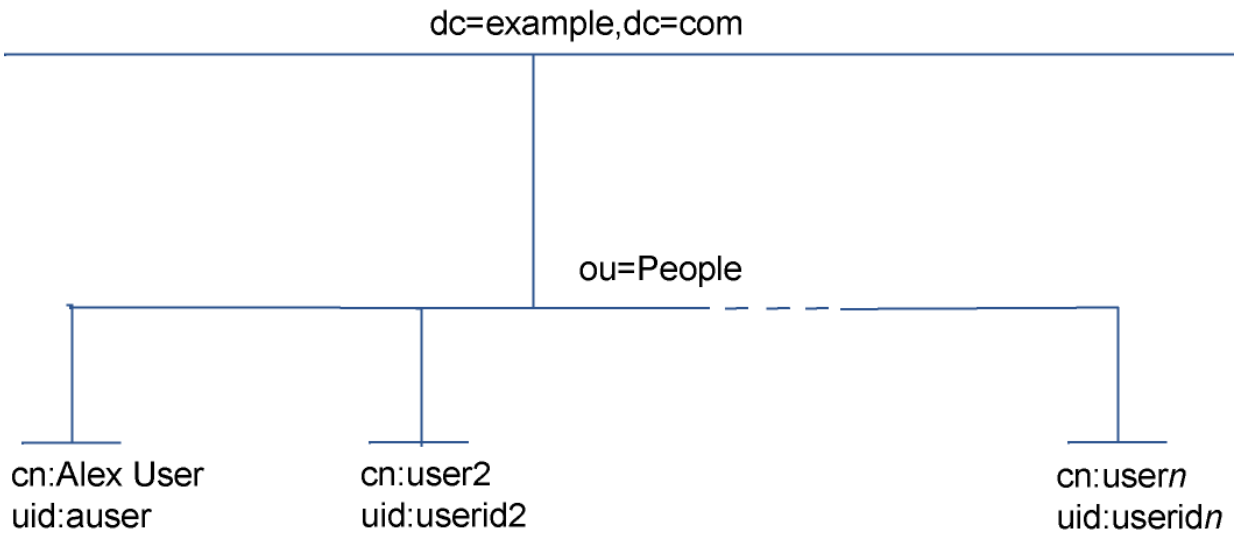
LDAP directory organization

To configure your FortiGate unit to work with an LDAP server, you need to understand the organization of the information on the server.

The top of the hierarchy is the organization itself. Usually this is defined as Domain Component (DC), a DNS domain. If the name contains a dot, such as `example.com`, it is written as two parts separated by a comma: `dc=example,dc=com`.

In this example, Common Name (CN) identifiers reside at the Organization Unit (OU) level, just below DC. The Distinguished Name (DN) is ou=People,dc=example,dc=com.

LDAP object hierarchy



In addition to the DN, the FortiGate unit needs an identifier for the individual person. Although the FortiGate unit GUI calls this the Common Name (CN), the identifier you use is not necessarily CN. On some servers, CN is the full name of a person. It might be more convenient to use the same identifier used on the local computer network. In this example, User ID (UID) is used.

Locating your identifier in the hierarchy

You need to determine the levels of the hierarchy from the top to the level that contain the identifier you want to use. This defines the DN that the FortiGate unit uses to search the LDAP database. Frequently used distinguished name elements include:

- uid (user identification)
- pw (password)
- cn (common name)
- ou (organizational unit)
- o (organization)
- c (country)

One way to test this is with a text-based LDAP client program. For example, OpenLDAP includes a client, `ldapsearch`, that you can use for this purpose.

Enter the following at the command line:

```
ldapsearch -x '(objectclass=*)'
```

The output is lengthy, but the information you need is in the first few lines:

```
version: 2
#
# filter: (objectclass=*)
# requesting: ALL

dn: dc=example,dc=com
dc: example
objectClass: top
objectClass: domain

dn: ou=People,dc=example,dc=com
ou: People
objectClass: top
objectClass: organizationalUnit
...
dn: uid=tbrown,ou=People,dc=example,dc=com
uid: tbrown
cn: Tom Brown
```

In the output above, you can see `tbrown` (uid) and `Tom Brown`(cn). Also note the dn is `ou=People, dc=example, dc=com`.

Configuring the FortiGate unit to use an LDAP server

After you determine the common name and distinguished name identifiers and the domain name or IP address of the LDAP server, you can configure the server on the FortiGate unit. The maximum number of remote LDAP servers that can be configured is 10.

One or more servers must be configured on FortiGate before remote users can be configured. To configure remote users, see Local and remote users on page 47.

To configure the FortiGate unit for LDAP authentication - web-based manager:

1. Go to **User & Device > Authentication > LDAP Servers** and select **Create New**.
2. Enter a **Name** for the LDAP server.
3. In **Server Name/IP** enter the server's FQDN or IP address.
4. If necessary, change the **Server Port** number. The default is port 389.
5. Enter the **Common Name Identifier** (20 characters maximum).
   `cn` is the default, and is used by most LDAP servers.
6. In the **Distinguished Name** field, enter the base distinguished name for the server using the correct X.500 or LDAP format.
   The FortiGate unit passes this distinguished name unchanged to the server. The maximum number of characters is 512.
   If you don't know the distinguished name, leave the field blank and select the Query icon to the right of the field.
   See Using the Query icon on page 32.
7. In the **Distinguished Name** field, enter the base distinguished name for the server using the correct X.500 or LDAP format.
   The FortiGate unit passes this distinguished name unchanged to the server. The maximum number of characters is 512.
   If you don't know the distinguished name, leave the field blank and select the Query icon to the right of the field.
   See Using the Query icon on page 32.
8. In **Bind Type**, select **Regular**.
9. In **User DN**, enter the LDAP administrator's distinguished name.
10. In **Password**, enter the LDAP administrator's password.
11. Select **OK**.

To verify your Distinguished Name field is correct, you can select the **Test** button. If your DN field entry is valid, you will see the part of the LDAP database it defines. If your DN field entry is not valid, it will display an error message and return no information.

For detailed information about configuration options for LDAP servers, see the Online Help on your FortiGate unit or the FortiGate CLI Reference.

To configure the FortiGate unit for LDAP authentication - CLI example:

```
config user ldap
   edit ourLDAPsrv
      set server 10.11.101.160
      set cnid cn
      set dn cn=users,dc=office,dc=example,dc=com
      set type regular
      set username cn=administrator,cn=users,dc=office,dc=example,dc=com
      set password w5AiGVMLkgyPQ
      set password-expiry-warning enable
      set password-renewal enable
   end
```

password-expiry-warning and password-renewal

In SSLVPN, when an LDAP user is connecting to the LDAP server it is possible for them to receive any pending password expiry or renewal warnings. When the password renewal or expiry warning exists, SSLVPN users will see a prompt allowing them to change their password.

`password-expiry-warning` allows FortiOS to detect from the LDAP server when a password is expiring or has expired using server controls or error codes.

`password-renewal` allows FortiOS to perform the online LDAP password renewal operations the LDAP server expects.

On an OpenLDAP server, when a user attempts to logon with an expired password they are allowed to logon but only to change their password.

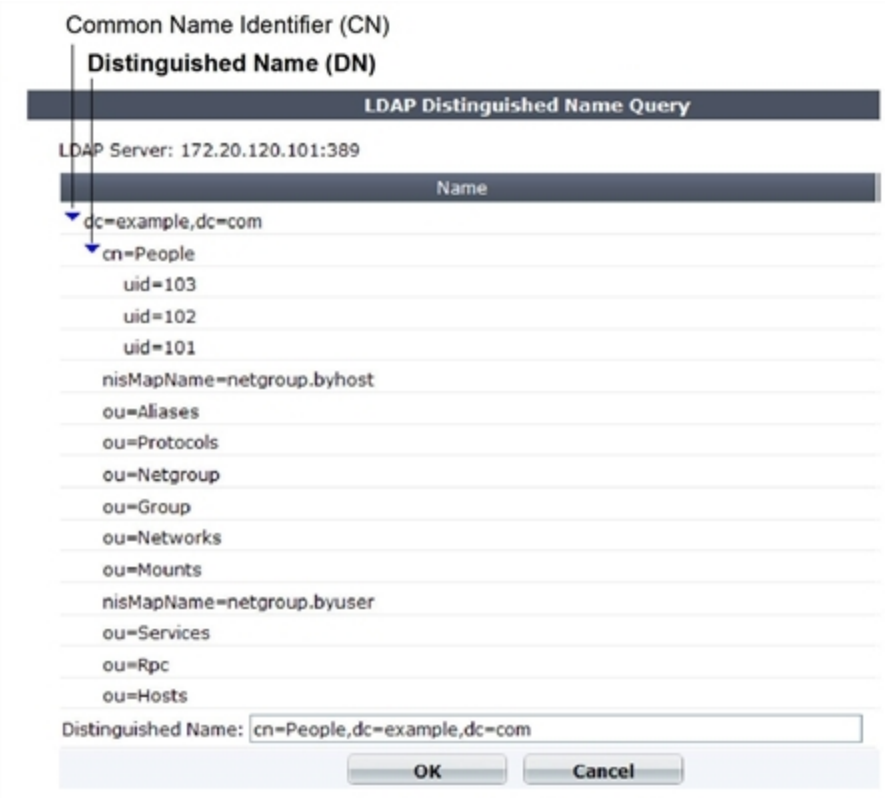
When changing passwords on a Windows AD system, the connection must be SSL-protected.

Using the Query icon

The LDAP Distinguished Name Query list displays the LDAP directory tree for the LDAP server connected to the FortiGate unit. This helps you to determine the appropriate entry for the DN field. To see the distinguished name associated with the Common Name identifier, select the Expand icon next to the CN identifier. Select the DN from the list. The DN you select is displayed in the Distinguished Name field. Select OK and the Distinguished Name you selected will be saved in the Distinguished Name field of the LDAP Server configuration.

To see the users within the LDAP Server user group for the selected Distinguished Name, expand the Distinguished Name in the LDAP Distinguished Name Query tree.

LDAP server Distinguished Name Query tree



Example — wildcard admin accounts - CLI

A wildcard admin account is an administrator account with the wildcard option enabled. This option allows multiple different remote administration accounts to match one local administration account, avoiding the need to set up individual admin accounts on the FortiGate unit. Instead multiple LDAP admin accounts will all be able to use one FortiGate admin account.

The initial benefit of wildcard admin accounts is fast configuration of the FortiGate unit's administration account to work with your LDAP network. The many to one ratio saves on effort, and potential errors.

The ongoing benefit is that as long as the users on the LDAP system belong to that group, and the test admin user settings don't change on the FortiGate unit, no other work is required. This point is important as it can help avoid system updates or changes that would otherwise require changes to the LDAP administrator account configuration. Even if a user is added to or removed from the LDAP group, no changes are required on the FortiGate unit.

Two potential issues with wildcard admin accounts are that multiple users may be logged on to the same account at the same time. This becomes an issue if they are changing the same information at the same time. The other potential issue is that security is reduced because multiple people have login access for the same account. If each user was assigned their own account, a hijacking of one account would not affect the other users.

Note that wildcard admin configuration also applies to RADIUS. When configuring for RADIUS, configure the RADIUS server, and RADIUS user group instead of LDAP. When using web-based management, wildcard admin is the only type of remote administrator account that does not require you to enter a password on account

creation. That password is normally used when the remote authentication server is unavailable during authentication.

In this example, default values are used where possible. If a specific value is not mentioned, it is set to its default value.

Configuring the LDAP server

The important parts of this configuration are the username and group lines. The username is the domain administrator account. The group binding allows only the group with the name `GRP` to access.

The `dn` used here is as an example only. On your network use your own domain name.

To configure LDAP server - CLI:

```
config user ldap
   edit "ldap_server"
      set server "192.168.201.3"
      set cnid "sAMAccountName"
      set dn "DC=example,DC=com,DC=au"
      set type regular
      set username "CN=Administrator,CN=Users,DC=example,DC=COM”
      set password *
      set group-member-check group-object
      set group-object-filter (&(objectcategory=group)
          member="CN=GRP,OU=training,DC=example,DC=COM"))
   next
end
```

To configure the user group and add the LDAP server - CLI:

```
config user group
   edit "ldap_grp"
      set member "ldap"
         config match
            edit 1
               set server-name "ldap_server"
               set group-name "CN=GRP,OU=training,DC=example,DC=COM"
            next
         end
      next
   end
```

Configuring the admin account

The wildcard part of this example is only available in the CLI for admin configuration. When enabled, this allows all LDAP group members to login to the FortiGate unit without the need to create a separate admin account for each user. In effect the members of that group will each be able to login as “test”.

To configure the admin account - CLI:

```
config system admin
```

```
   edit "test"
      set remote-auth enable
      set accprofile "super_admin"
      set wildcard enable
      set remote-group "ldap_grp"
   next
end
```

For troubleshooting, test that the admin account is operational, and see Troubleshooting LDAP on page 36.

Example of LDAP to allow Dial-in through member-attribute - CLI

In this example, users defined in MicroSoft Windows Active Directory (AD) are allowed to setup a VPN connection simply based on an attribute that is set to TRUE, instead of based on being part of a specific group.

In AD, the “Allow Dial-In” property is activated in the user properties, and this sets the `msNPAllowDialin` attribute to “TRUE”.

This same procedure can be used for other member attributes, as your system requires.

Configuring LDAP member-attribute settings

To accomplish this with a FortiGate unit, the member attribute must be set. Setting member attributes can only be accomplished through the CLI using the `member-attr` keyword - the option is not available through the web-based manager.

Before configuring the FortiGate unit, the AD server must be configured and have the `msNPAllowDialin` attribute set to “TRUE” for the users in question. If not, those users will not be able to properly authenticate.

The dn used here is as an example only. On your network use your own domain name.

To configure user LDAP member-attribute settings - CLI:

```
config user ldap
   edit "ldap_server"
      set server "192.168.201.3"
      set cnid "sAMAccountName"
      set dn "DC=fortinet,DC=com,DC=au"
      set type regular
      set username "fortigate@example.com"
      set password ******
      set member-attr "msNPAllowDialin"
   next
end
```

Configuring LDAP group settings

A user group that will use LDAP must be configured. This example adds the member `ldap` to the group which is the LDAP server name that was configured earlier.

To configure LDAP group settings - CLI:

```
config user group
   edit "ldap_grp"
      set member "ldap"
      config match
```

```
        edit 1
           set server-name "ldap"
           set group-name "TRUE"
        next
     end
end
```

Once these settings are in place, users can authenticate.

Troubleshooting LDAP

The examples in this section use the values from the previous example.

LDAP user test

A quick way to see if the LDAP configuration is correct is to run a diagnose CLI command with LDAP user information. The following command tests with a user called `netAdmin` and a password of `fortinet`. If the configuration is correct the test will be successful.

```
FGT# diag test authserver ldap ldap_server netAdmin fortinet
```

`'ldap_server' is not a valid ldap server name` — an LDAP server by that name has not been configured on the FortiGate unit, check your spelling.

`authenticate 'netAdmin' against 'ldap_server' failed!` — the user `netAdmin` does not exist on `ldap_server`, check your spelling of both the user and sever and ensure the user has been configured on the FortiGate unit.

LDAP authentication debugging

For a more in-depth test, you can use a `diag debug` command. The sample output from a shows more information about the authentication process that may prove useful if there are any problems.

Ensure the “Allow Dial-in” attribute is still set to “TRUE” and run the following CLI command. `fnbamd` is the Fortinet non-blocking authentication daemon.

```
FGT# diag debug enable
FGT# diag debug reset
FGT# diag debug application fnbamd -1
FGT# diag debug enable
```

The output will look similar to:

```
get_member_of_groups-Get the memberOf groups.
get_member_of_groups- attr='msNPAllowDialin', found 1 values
get_member_of_groups-val[0]='TRUE'
fnbamd_ldap_get_result-Auth accepted
fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth_poll_ldap-Result for ldap svr 192.168.201.3 is SUCCESS
fnbamd_auth_poll_ldap-Passed group matching
```

If the “Allow Dial-in” attribute is not set but it is expected, the last line of the above output will instead be:

```
fnbamd_auth_poll_ldap-Failed group matching
```

TACACS+ servers

When users connect to their corporate network remotely, they do so through a remote access server. As remote access technology has evolved, the need for security when accessing networks has become increasingly important. This need can be filled using a Terminal Access Controller Access-Control System (TACACS+) server.

TACACS+ is a remote authentication protocol that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ allows a client to accept a username and password and send a query to a TACACS+ authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies the user access to the network.

TACACS+ offers fully encrypted packet bodies, and supports both IP and AppleTalk protocols. TACACS+ uses TCP port 49, which is seen as more reliable than RADIUS's UDP protocol.

There are several different authentication protocols that TACACS+ can use during the authentication process:

Authentication protocols

Protocol	Definition
ASCII	Machine-independent technique that uses representations of English characters. Requires user to type a username and password that are sent in clear text (unencrypted) and matched with an entry in the user database stored in ASCII format.
PAP	Password Authentication Protocol (PAP) Used to authenticate PPP connections. Transmits passwords and other user information in clear text.
CHAP	Challenge-Handshake Authentication Protocol (CHAP) Provides the same functionality as PAP, but is more secure as it does not send the password and other user information over the network to the security server.
MS-CHAP	MicroSoft Challenge-Handshake Authentication Protocol v1 (MSCHAP) Microsoft-specific version of CHAP.
default	The default protocol configuration, Auto, uses PAP, MS-CHAP, and CHAP, in that order.

Configuring a TACACS+ server on the FortiGate unit

A maximum of 10 remote TACACS+ servers can be configured for authentication.

One or more servers must be configured on FortiGate before remote users can be configured. To configure remote users, see Local and remote users on page 47.

The TACACS+ page in the web-based manager is not available until a TACACS+ server has been configured in the CLI. For more information see the CLI Reference.

To configure the FortiGate unit for TACACS+ authentication - web-based manager:

1. Go to **User & Device > Authentication > TACACS+ Servers** and select **Create New**.
2. Enter the following information, and select **OK**.

Name	Enter the name of the TACACS+ server.
Server Name/IP	Enter the server domain name or IP address of the TACACS+ server.
Server Key	Enter the key to access the TACACS+ server.
Authentication Type	Select the authentication type to use for the TACACS+ server. **Auto** tries PAP, MSCHAP, and CHAP (in that order).

To configure the FortiGate unit for TACACS+ authentication - CLI:

```
config user tacacs+
   edit tacacs1
      set authen-type auto
      set key abcdef
      set port 49
      set server 192.168.0.101
   end
```

POP3 servers

FortiOS can authenticate users who have accounts on POP3 or POP3s email servers. POP3 authentication can be configured only in the CLI.

To configure the FortiGate unit for POP3 authentication:

```
config user pop3
   edit pop3_server1
      set server pop3.fortinet.com
      set secure starttls
      set port 110
   end
```

To configure a POP3 user group:

```
config user group
   edit pop3_grp
      set member pop3_server1
   end
```

A user group can list up to six POP3 servers as members.

SSO servers

Novell and Microsoft Windows networks provide user authentication based on directory services: eDirectory for Novell, Active Directory for Windows. Users can log on at any computer in the domain and have access to resources as defined in their user account. The Fortinet Single Sign On (FSSO) agent enables FortiGate units to authenticate these network users for security policy or VPN access without asking them again for their username and password.

When a user logs in to the Windows or Novell domain, the FSSO agent sends to the FortiGate unit the user's IP address and the names of the user groups to which the user belongs. The FortiGate unit uses this information to maintain a copy of the domain controller user group database. Because the domain controller authenticates users, the FortiGate unit does not perform authentication. It recognizes group members by their IP address.

In the FortiOS FSSO configuration, you specify the server where the FSSO Collector agent is installed. The Collector agent retrieves the names of the Novell or Active Directory user groups from the domain controllers on the domains, and then the FortiGate unit gets them from the Collector agent. You cannot use these groups directly. You must define FSSO type user groups on your FortiGate unit and then add the Novell or Active Directory user groups to them. The FSSO user groups that you created are used in security policies and VPN configurations to provide access to different services and resources.

FortiAuthenticator servers can replace the Collector agent when FSSO is using polling mode. The benefits of this is that FortiAuthenticator is a stand-alone server that has the necessary FSSO software pre-installed. For more information, see the FortiAuthenticator Administration Guide.

Single Sign-on Agent configuration settings

The following are SSO configuration settings in **User & Device > Authentication > Single Sign-On**.

SSO Server List

Lists all the collector agents' lists that you have configured. On this page, you can create, edit or delete FSSO agents. There are different types of FSSO agents, each with its own settings.

Note: You can create a redundant configuration on your unit if you install a collector agent on two or more domain controllers. If the current (or first) collector agent fails, the Fortinet unit switches to the next one in its list of up to five collector agents.

Create New	Creates a new agent. When you select **Create New**, you are automatically redirected to the New page.
Edit	Modifies the settings for the selected SSO server. To remove multiple entries from the list, for each servers you want removed, select the check box and then select **Delete**. To remove all agents from the list, on the FSSO Agent page, select the check box at the top of the check box column and then select **Delete**.
Delete	Removes an agent from the list on the page.

Settings when Type is Poll Active Directory Server	
Server IP/Name	The IP address of the domain controller (DC).
User	The user ID used to access the domain controller.
Password	Enter the password for the account used to access the DC.
LDAP Server	Select the check box and select an LDAP server to access the Directory Service.
Enable Polling	Enable to allow the FortiGate unit to poll this DC.
Users/Groups	A list of user and user group names retrieved from the DC.

Settings when Type is Fortinet Single Sign On Agent	
Name	Enter a name for the SSO server.
Primary Agent IP/Name **Secondary Agent IP/Name**	Enter the IP address or name of the Directory Service server where this SSO agent is installed. The maximum number of characters is 63.
Password	Enter the password for the collector agent. This is required only if you configured your Fortinet Single Sign On Agent collector agent to require authenticated access.
LDAP Server	Select the check box and select an LDAP server to access the Directory Service.
More FSSO agents	Select to add up to three additional SSO agents.
Users/Groups	A list of user and user group names retrieved from the server.

Settings when Type is RADIUS Single Sign On Agent	
Use RADIUS Shared Secret	Enable
Shared Secret	Enter the RADIUS server shared secret.
Send RADIUS Responses	Enable.

RSA ACE (SecurID) servers

SecurID is a two-factor system that uses one-time password (OTP) authentication. It is produced by the company RSA. This system includes portable tokens carried by users, an RSA ACE/Server, and an Agent Host. In our

configuration, the FortiGate unit is the Agent Host.

Components

When using SecurID, users carry a small device or "token" that generates and displays a pseudo-random password. According to RSA, each SecurID authenticator token has a unique 64-bit symmetric key that is combined with a powerful algorithm to generate a new code every 60 seconds. The token is time-synchronized with the SecurID RSA ACE/Server.

The RSA ACE/Server is the management component of the SecurID system. It stores and validates the information about the SecurID tokens allowed on your network. Alternately the server could be an RSA SecurID 130 Appliance.

The Agent Host is the server on your network, in this case it is the FortiGate unit, that intercepts user logon attempts. The Agent Host gathers the user ID and password entered from their SecurID token, and sends that information to the RSA ACE/Server to be validated. If valid, a reply comes back indicating it is a valid logon and the FortiGate unit allows the user access to the network resources specified in the associated security policy.

Configuring the SecurID system

To use SecurID with a FortiGate unit, you need:

- to configure the RSA server and the RADIUS server to work with each other (see RSA server documentation)
- to configure the RSA SecurID 130 Appliance
  or
- to configure the FortiGate unit as an Agent Host on the RSA ACE/Server
- to configure the FortiGate unit to use the RADIUS server
- to create a SecurID user group
- to configure a security policy with SecurID authentication

The following instructions are based on RSA ACE/Server version 5.1, or RSA SecurID 130 Appliance, and assume that you have successfully completed all the external RSA and RADIUS server configuration steps listed above.

For this example, the RSA server is on the internal network, with an IP address of 192.128.100.100. The FortiGate unit internal interface address is 192.168.100.3, RADIUS shared secret is fortinet123, RADIUS server is at IP address 192.168.100.102.

To configure the RSA SecurID 130 Appliance

1. Go to the IMS Console for SecurID and logon.
2. Go to **RADIUS > RADIUS Clients**, and select **Add New.**
3. Enter the following information to configure your FortiGate as a SecurID Client, and select Save.

RADIUS Client Basics	
Client Name	FortiGate
Associated RSA Agent	FortiGate

RADIUS Client Settings	
IP Address	192.168.100.3 The IP address of the FortiGate unit internal interface.
Make / Model	Select Standard Radius
Shared Secret	fortinet123 The RADIUS shared secret.
Accounting	Leave unselected
Client Status	Leave unselected

To configure the FortiGate unit as an Agent Host on the RSA ACE/Server

1. On the RSA ACE/Server computer, go to **Start > Programs > RSA ACE/Server**, and then **Database Administration - Host Mode**.
2. On the **Agent Host** menu, select **Add Agent Host**.
3. Enter and save the following information.

Name	FortiGate
Network Address	192.168.100.3 The IP address of the FortiGate unit.
Secondary Nodes	Optionally enter other IP addresses that resolve to the FortiGate unit.

If needed, refer to the RSA ACE/Server documentation for more information.

To configure the FortiGate unit to use the RADIUS server

1. Go to **User & Device > Authentication > RADIUS Servers** and select **Create New**.
2. Enter the following information, and select **OK**.

Name	RSA
Primary Server IP/Name	192.168.100.102 Optionally select Test to ensure the IP address is correct and the FortiGate can contact the RADIUS server.
Primary Server Secret	fortinet123
Authentication Scheme	Select **Use Default Authentication Scheme**.

To create a SecurID user group

1. Go to **User & Device > User > User Groups**, and select **Create New**.
2. Enter the following information.

Name	RSA_group
Type	Firewall

3. In **Remote Groups**, select **Add**, then select the RSA server.
4. Select **OK**.

To create a SecurID user:

1. Go to **User & Device > User > User Definition**, and select **Create New**.
2. Use the wizard to enter the following information, and then select **Create**.

User Type	Remote RADIUS User
User Name	wloman
RADIUS Server	RSA
Contact Info	(optional) Enter Email or SMS information
User Group	RSA_group

To test this configuration, on your FortiGate unit use the CLI command:

```
diagnose test authserver radius RSA auto wloman 111111111
```

The series of 1s is the one time password that your RSA SecurID token generates and you enter.

Using the SecurID user group for authentication

You can use the SecurID user group in several FortiOS features that authenticate by user group including

- Security policy
- IPsec VPN XAuth
- PPTP VPN
- SSL VPN

The following sections assume the SecurID user group is called `securIDgrp` and has already been configured. Unless otherwise states, default values are used.

Security policy

To use SecurID in a security policy, you must include the SecurID user group in a security policy. This procedure will create a security policy that allows HTTP, FTP, and POP3 traffic from the `internal` interface to `wan1`. If these interfaces are not available on your FortiGate unit, substitute other similar interfaces.

To configure a security policy with SecurID authentication

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select **Create New**.
3. Enter:

Incoming Interface	internal
Source Address	all
Source User(s)	securIDgrp
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Services	HTTP, FTP, POP3
Action	ACCEPT
NAT	On
Shared Shaper	On, if you want to either limit traffic or guarantee minimum bandwidth for traffic that uses the SecurID security policy. Use the default shaper **guarantee-100kbps**.
Log Allowed Traffic	On, if you want to generate usage reports on traffic authenticated with this policy.

4. Select **OK**.
   The SecurID security policy is configured.

For more detail on configuring security policies, see the FortiOS Handbook FortiGate Fundamentals guide.

IPsec VPN XAuth

Extended Authentication (XAuth) increases security by requiring user authentication in addition to the preshared key.

When creating an IPsec VPN using the wizard (**VPN > IPsec > Wizard**), select the SecurID **User Group** on the Authentication page. Members of the SecurID group are required to enter their SecureID code to authenticate.

For more on XAuth, see Configuring XAuth authentication on page 83

PPTP VPN

PPTP VPN is configured in the CLI. In the PPTP configuration (`config vpn pptp`), set `usrgrp` to the SecurID user group.

SSL VPN

You need to map the SecurID user group to the portal that will serve SecurID users and include the SecurID user group in the **Source User(s)** field in the security policy.

To map the SecurID group to an SSL VPN portal:

1. Go to **VPN > SSL > Settings**.
2. In **Authentication/Portal Mapping**, select **Create New**.
3. Enter

Users/Groups	securIDgrp
Portal	Choose the portal.

4. Select **OK**.

Users and user groups

FortiGate authentication controls system access by user group. By assigning individual users to the appropriate user groups you can control each user's access to network resources. The members of user groups are user accounts, of which there are several types. Local users and peer users are defined on the FortiGate unit. User accounts can also be defined on remote authentication servers.

This section describes how to configure local users and peer users and then how to configure user groups. For information about configuration of authentication servers see Authentication servers on page 22.

This section contains the following topics:

Users

A user is a user account consisting of username, password, and in some cases other information, configured on the FortiGate unit or on an external authentication server. Users can access resources that require authentication only if they are members of an allowed user group. There are several different types of user accounts with slightly different methods of authentication:

User type	Authentication
Local user	The username and password must match a user account stored on the FortiGate unit. Authentication by FortiGate security policy.
Remote user	The username must match a user account stored on the FortiGate unit and the username and password must match a user account stored on the remote authentication server. FortiOS supports LDAP, RADIUS, and TACACS+ servers.
Authentication server user	A FortiGate user group can include user accounts or groups that exist on a remote authentication server.
FSSO user	With Fortinet Single Sign On (FSSO), users on a Microsoft Windows or Novell network can use their network authentication to access resources through the FortiGate unit. Access is controlled through FSSO user groups which contain Windows or Novell user groups as their members.
PKI or Peer user	A Public Key Infrastructure (PKI) or peer user is a digital certificate holder who authenticates using a client certificate. No password is required, unless two-factor authentication is enabled.
IM Users	IM users are not authenticated. The FortiGate unit can allow or block each IM user name from accessing the IM protocols. A global policy for each IM protocol governs access to these protocols by unknown users.

User type	Authentication
Guest Users	Guest user accounts are temporary. The account expires after a selected period of time.

This section includes:

Local and remote users

Local and remote users are defined on the FortiGate unit in **User & Device > User > User Definition**.

Create New	Creates a new user account. When you select **Create New**, you are automatically redirected to the User Creation Wizard.
Edit User	Modifies a user's account settings. When you select **Edit**, you are automatically redirected to the Edit User page.
Delete	Removes a user from the list. Removing the user name removes the authentication configured for the user. The **Delete** icon is not available if the user belongs to a user group. To remove multiple local user accounts from within the list, on the User page, in each of the rows of user accounts you want removed, select the check box and then select **Delete**. To remove all local user accounts from the list, on the User page, select the check box in the check box column and then select **Delete**.
User Name	The user name. For a remote user, this username must be identical to the username on the authentication server.
Type	Local indicates a local user authenticated on the FortiGate unit. For remote users, the type of authentication server is shown: LDAP, RADIUS, or TACACS+.
Two-factor Authentication	Indicates whether two-factor authentication is configured for the user.

Ref.	Displays the number of times this object is referenced by other objects. Select the number to open the Object Usage window and view the list of referring objects. The list is grouped into expandable categories, such as Firewall Policy. Numbers of objects are shown in parentheses. To view more information about the referring object, use the icons: • **View the list page for these objects** – available for object categories. Goes to the page where the object is listed. For example, if the category is User Groups, opens User Groups list. • **Edit this object** – opens the object for editing. • **View the details for this object** – displays current settings for the object.

To create a local or remote user account - web-based manager:

1. Go to **User & Device > User > User Definition** and select **Create New**.
2. On the **Choose User Type** page select:

Local User	Select to authenticate this user using a password stored on the FortiGate unit.
Remote RADIUS User **Remote TACACS+ User** **Remote LDAP User**	To authenticate this user using a password stored on an authentication server, select the type of server and then select the server from the list. You can select only a server that has already been added to the FortiGate unit configuration.

3. Select **Next** and provide user authentication information.
   For a local user, enter the **User Name** and **Password**.
   For a remote user, enter the **User Name** and the server name.
4. Select **Next** and enter **Contact Information**.
   If email or SMS is used for two-factor authentication, provide the email address or SMS cell number at which the user will receive token password codes. If a custom SMS service is used, it must already be configured in **System > Config > Advanced >SMS Service**. See FortiToken on page 53.
5. Select **Next**, then on the **Provide Extra Info** page enter

Two-factor Authentication	Select to enable two-factor authentication. Then select the Token (FortiToken or FortiToken Mobile) for this user account. See Associating FortiTokens with accounts on page 57.
User Group	Select the user groups to which this user belongs.

6. Select **Create**.

To create a local user - CLI example:

Locally authenticated user

```
config user local
   edit user1
      set type password
      set passwd ljt_pj2gpepfdw
   end
```

To create a remote user - CLI example:

```
config user local
   edit user2
      set type ldap
      set ldap_server ourLDAPsrv
   end
```

For a RADIUS or TACACS+ user, set `type` to `radius` or `tacacs+`, respectively.

To create a user with FortiToken Mobile two-factor authentication - CLI example:

```
config user local
   edit user5
      set type password
      set passwd ljt_pj2gpepfdw
      set two_factor fortitoken
      set fortitoken 182937197
   end
```

Remote users are configured for FortiToken two-factor authentication similarly.

To create a user with SMS two-factor authentication using FortiGuard messaging Service - CLI example:

```
config user local
   edit user6
      set type password
      set passwd 3ww_pjt68dw
      set two_factor sms
      set sms-server fortiguard
      set sms-phone 1365984521
   end
```

Removing users

Best practices dictate that when a user account is no longer in use, it should be deleted. Removing local and remote users from FortiOS involve the same steps.

If the user account is referenced by any configuration objects, those references must be removed before the user can be deleted. See Removing references to users on page 50.

To remove a user from the FortiOS configuration - web-based manager:

1. Go to **User & Device > User > User Definition**.
2. Select the check box of the user that you want to remove.
3. Select **Delete**.
4. Select **OK**.

To remove a user from the FortiOS configuration - CLI example:

```
config user local
   delete user4444
end
```

Removing references to users

You cannot remove a user that belongs to a user group. Remove the user from the user group first, and then delete the user.

To remove references to a user - web-based manager

1. Go to **User & Device > User > User Definition**.
2. If the number in the far right column for the selected user contains any number other than zero, select it.
3. A more detailed list of object references to this user is displayed. Use its information to find and remove these references to allow you to delete this user.

PKI or peer users

A PKI, or peer user, is a digital certificate holder. A PKI user account on the FortiGate unit contains the information required to determine which CA certificate to use to validate the user's certificate. Peer users can be included in firewall user groups or peer certificate groups used in IPsec VPNs. For more on certificates, see Certificates overview on page 96.

To define a peer user you need:

- a peer username
- the text from the subject field of the user's certificate, or the name of the CA certificate used to validate the user's certificate

Creating a peer user

The peer user can be configured only in the CLI.

To create a peer user for PKI authentication - CLI example:

```
config user peer
   edit peer1
      set subject peer1@mail.example.com
      set ca CA_Cert_1
   end
```

There are other configuration settings that can be added or modified for PKI authentication. For example, you can configure the use of an LDAP server to check access rights for client certificates. For information about the detailed PKI configuration settings, see the FortiGate CLI Reference.

Two-factor authentication

The standard logon requires a username and password. This is one factor authentication—your password is one piece of information you need to know to gain access to the system.

Two factor authentication adds the requirement for another piece of information for your logon. Generally the two factors are something you know (password) and something you have (certificate, token, etc.). This makes it harder for a hacker to steal your logon information. For example if you have a FortiToken device, the hacker would need to both use it and know your password to gain entry to your account.

Two-factor authentication is available on both user and admin accounts. But before you enable two-factor authentication on an administrator account, you need to ensure you have a second administrator account configured to guarantee administrator access to the FortiGate unit if you are unable to authenticate on the main admin account for some reason.

Two-factor authentication does not work with explicit proxies.

The methods of two-factor authentication include:

- Certificate
- Email
- SMS
- FortiToken

Certificate

You can increase security by requiring both certificate and password authentication for PKI users. Certificates are installed on the user's computer. Requiring a password also protects against unauthorized use of that computer.

Optionally peer users can enter the code from their FortiToken instead of the certificate.

To create a peer user with two-factor authentication - CLI example

```
config user peer
   edit peer1
      set subject E=peer1@mail.example.com
      set ca CA_Cert_1
      set two-factor enable
      set passwd fdktguefheygfe
   end
```

For more information on certificates, see Certificates overview on page 96.

Email

Two-factor email authentication sends a randomly generated six digit numeric code to the specified email address. Enter that code when prompted at logon. This token code is valid for 60 seconds. If you enter this code after that time,it will not be accepted.

A benefit is that you do not require mobile service to authenticate. However, a potential issue is if your email server does not deliver the email before the 60 second life of the token expires.

The code will be generated and emailed at the time of logon, so you must have email access at that time to be able to receive the code.

To configure an email provider - web-based manager:

1. Go to **System > Config > Advanced > Email Service**.
2. Enter **SMTP Server** and **Default Reply To** address.
3. If applicable, enable **Authentication** and enter the **SMTP User** and **Password** to use.

4. Select a **Security Mode**, options are: **None**, **SMTPS** or **STARTTLS**.
5. Enter the **Port** number, the default is 25.
6. Select **Apply**.

To configure an email provider - CLI:

```
config system email-server
   set server <server_domain-name>
   set reply-to <Recipient_email_address>
end
```

To enable email two-factor authentication - web-based manager:

1. To modify an administrator account, go to **System > Admin > Administrators**. To modify a user account go to **User & Device > User > User Definition**.
2. Edit the user account.
3. Enable and enter the user's **Email Address**.
4. Select **Enable Two-factor Authentication**.
5. Select **Email based two-factor authentication**.
6. Select **OK**.

If **Email based two-factor authentication** option doesn't appear after selecting **Enable Two-factor Authentication**, you need to enable it via the CLI as follows.

To enable email two-factor authentication - CLI:

```
config user local
   edit <user_name>
      set email-to <user_email>
      set two-factor email
   end
```

SMS

SMS two-factor authentication sends the token code in an SMS text message to the mobile device indicated when this user attempts to logon. This token code is valid for 60 seconds. If you enter this code after that time, it will not be accepted. Enter this code when prompted at logon to be authenticated.

SMS two-factor authentication has the benefit that you do not require email service before logging on. A potential issue is if the mobile service provider does not send the SMS text message before the 60 second life of the token expires.

FortiGuard Messaging Service include 4 SMS Messages at no cost. If you need more, you should acquire a license through support.fortinet.com or via customer service.

If you do not use the FortiGuard Messaging Service, you need to configure an SMS service.

To configure an SMS service for your FortiGate unit - web-based manager:

1. Go to **System > Config > Advanced**.
2. In **SMS Service**, select **Create New**.
3. Enter a **Name** for the SMS service and the service **Address** (domain name), then select **OK**.
4. Select **Apply**.

To configure an SMS service - CLI:

```
config system sms-server
   edit <provider_name>
      set mail-server <server_domain-name>
   next
end
```

To configure SMS two-factor authentication - web-based manager:

1. To modify an:
   - administrator account, go to **System > Admin > Administrators, or**
   - user account go to **User & Device > User > User Definition**.
2. Edit the user account.
3. Select SMS and either:
   - Select **FortiGuard Messaging Service**
     or
   - Select **Custom** and then choose the **SMS Provider** to use.
4. Select the **Country/Region**.
5. Enter the phone number of the mobile device that will receive the SMS text messages.
6. Select **Enable Two-factor Authentication**.
7. Select **SMS based two-factor authentication**.
8. Select **OK**.

If **SMS based two-factor authentication** option doesn't appear after selecting **Enable Two-factor Authentication**, you need to enable it via the CLI as follows.

To enable SMS two-factor authentication - CLI:

```
config user local
   edit <user_name>
      set sms-phone <user_phone>
      set sms-server fortiguard
      set two-factor sms
   end
```

If you have problems receiving the token codes via SMS messaging, contact your mobile provider to ensure you are using the correct phone number format to receive text messages and that your current mobile plan allows text messages.

FortiToken

FortiToken is a disconnected one-time password (OTP) generator. It is a small physical device with a button that when pressed displays a six digit authentication code. This code is entered with a user's username and password as two-factor authentication. The code displayed changes every 60 seconds, and when not in use the LCD screen is blanked to extend the battery life.

There is also a mobile phone application, FortiToken Mobile, that performs much the same function.

FortiTokens have a small hole in one end. This is intended for a lanyard to be inserted so the device can be worn around the neck, or easily stored with other electronic devices. Do not put the FortiToken on a key ring as the metal ring and other metal objects can damage it. The FortiToken is an electronic device like a cell phone and must be treated with similar care.

Any time information about the FortiToken is transmitted, it is encrypted. When the FortiGate unit receives the code that matches the serial number for a particular FortiToken, it is delivered and stored encrypted. This is in keeping with the Fortinet's commitment to keeping your network highly secured.

FortiTokens can be added to user accounts that are local, IPsec VPN, SSL VPN, and even Administrators. See Associating FortiTokens with accounts on page 57.

A FortiToken can be associated with only one account on one FortiGate unit.

If a user loses their FortiToken, it can be locked out using the FortiGate so it will not be used to falsely access the network. Later if found, that FortiToken can be unlocked on the FortiGate to allow access once again. See FortiToken maintenance on page 58.

There are three tasks to complete before FortiTokens can be used to authenticate accounts:

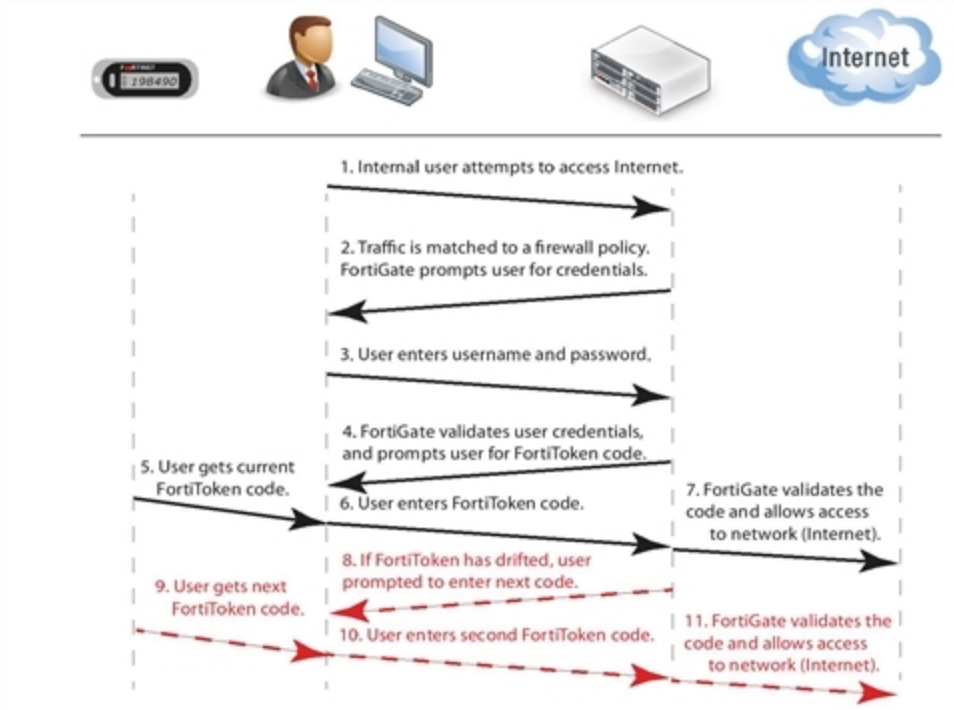
1. Adding FortiTokens to the FortiGate
2. Activating a FortiToken on the FortiGate
3. Associating FortiTokens with accounts

The FortiToken authentication process

The steps during FortiToken two-factor authentication are as follows.

1. User attempts to access a network resource.
2. FortiGate unit matches the traffic to an authentication security policy, and FortiGate unit prompts the user for username and password.
3. User enters their username and password.
4. FortiGate unit verifies their information, and if valid prompts the user for the FortiToken code.
5. User gets the current code from their FortiToken device.
6. User enters current code at the prompt.
7. FortiGate unit verifies the FortiToken code, and if valid allows access to the network resources such as the Internet.
   The following steps are needed only if the time on the FortiToken has drifted and needs to be re-synchronized with the time on the FortiGate unit.
8. If time on FortiToken has drifted, FortiGate unit will prompt user to enter a second code to confirm.
9. User gets the next code from their FortiToken device
10. User enters the second code at the prompt.
11. FortiGate unit uses both codes to update its clock to match the FortiToken and then proceeds as in step "Users and user groups" on page 46.

The FortiToken authentication process is illustrated below:



When configured the FortiGate unit accepts the username and password, authenticates them either locally or remotely, and prompts the user for the FortiToken code. The FortiGate then authenticates the FortiToken code. When FortiToken authentication is enabled, the prompt field for entering the FortiToken code is automatically added to the authentication screens.

Even when an Administrator is logging in through a serial or Telnet connection and their account is linked to a FortiToken, that Administrator will be prompted for the token's code at each login.

If you have attempted to add invalid FortiToken serial numbers, there will be no error message. The serial numbers will simply not be added to the list.

Adding FortiTokens to the FortiGate

Before one or more FortiTokens can be used to authenticate logons, they must be added to the FortiGate. The import feature is used to enter many FortiToken serial numbers at one time. The serial number file must be a text file with one FortiToken serial number per line.

One FortiToken can be added to multiple FortiGate units. This is useful for maintaining two-factor authentication for employees over multiple office locations, such as for employees who travel frequently between offices.

To manually add a FortiToken to the FortiGate - web-based manager:

1. Go to **User & Device > FortiTokens**.
2. Select **Create New**.
3. In **Type**, select **Hard Token** or **Mobile Token**.
4. Enter one or more FortiToken serial numbers (hard token) or activation codes (mobile token).
5. Select **OK**.

For mobile token, you receive the activation code in the license certificate once you purchase a license. FortiOS include a license for two mobile token at no cost.

To import multiple FortiTokens to the FortiGate - web-based manager:

1. Go to **User & Device > FortiTokens**.
2. Select **Create New**.
3. In **Type**, select **Hard Token**.
4. Select **Import**.
5. Select **Serial Number File** or **Seed File**, depending on which file you have.
6. Browse to the local file location on your local computer.
7. Select **OK**.
   The file is imported.
8. Select **OK**.

To add two FortiTokens to the FortiGate - CLI:

```
config user fortitoken
   edit <serial_number>
   next
   edit <serial_number2>
   next
end
```

Activating a FortiToken on the FortiGate

Once one or more FortiTokens have been added to the FortiGate unit, they must be activated before being available to be associated with accounts.The process of activation involves the FortiGate querying FortiGuard servers about the validity of each FortiToken. The serial number and information is encrypted before it is sent for added security.

A FortiGate unit requires a connection to FortiGuard servers to activate a FortiToken.

To activate a FortiToken on the FortiGate unit - web-based manager:

1. Go to **User & Device > FortiTokens**.
2. Select one or more FortiTokens with a status of Available.
3. Right-click the FortiToken entry and select **Activate**.
4. Select **Refresh**.
   The status of selected FortiTokens will change to Activated.

The selected FortiTokens are now available for use with user and admin accounts.

To activate a FortiToken on the FortiGate unit - CLI:

```
config user fortitoken
   edit <token_serial_num>
      set status activate
   next
end
```

Associating FortiTokens with accounts

The final step before using the FortiTokens to authenticate logons is associating a FortiToken with an account. The accounts can be local user or administrator accounts.

To add a FortiToken to a local user account - web-based manager:

1. Ensure that your FortiToken serial number has been added to the FortiGate successfully, and its status is Available.
2. Go to **User & Device > User > User Definition**, and edit the user account.
3. Select **Email Address** and enter user's email address.
4. Select **Enable Two-factor Authentication**.
5. Select the user's FortiToken serial number from the **Token** list.
6. Select **OK**.

For mobile token, click on **Send Activation Code**to be sent to the email address configured previously. The user will use this code to activate his mobile token. An **Email Service** has to be set under **System > Config > Advanced**in order to send the activation code.

To add a FortiToken to a local user account - CLI:

```
config user local
   edit <username>
      set type password
      set passwd "myPassword"
      set two-factor fortitoken
      set fortitoken <serial_number>
      set email-to "username@example.com"
      set status enable
   next
   end
```

To add a FortiToken to an administrator account - web-based manager:

1. Ensure that your FortiToken serial number has been added to the FortiGate successfully, and its status is Available.
2. Go to **System > Admin > Administrators**, and edit the admin account.
   This account is assumed to be configured except for two-factor authentication.
3. Select **Email Address** and enter admin's email address.
4. Select **Enable Two-factor Authentication**.

5. Select the user's FortiToken serial number from the **Token** list.
6. Select **OK**.

For mobile token, click on **Send Activation Code**to be sent to the email address configured previously. The admin will use this code to activate his mobile token. An **Email Service** has to be set under **System > Config > Advanced**in order to send the activation code.

To add a FortiToken to an administrator account - CLI:

```
config system admin
   edit <username>
      set password "myPassword"
      set two-factor fortitoken
      set fortitoken <serial_number>
      set email-to "username@example.com"
   next
   end
```

The `fortitoken` keyword will not be visible until `fortitoken` is selected for the `two-factor` option.

Before a new FortiToken can be used, it may need to be synchronized due to clock drift.

FortiToken maintenance

Once FortiTokens are entered into the FortiGate unit, there are only two tasks to maintain them — changing the status,

To change the status of a FortiToken between Activated and Locked - CLI:

```
config user fortitoken
   edit <token_serial_num>
      set status lock
   next
end
```

Any user attempting to login using this FortiToken will not be able to authenticate.

To list the drift on all FortiTokens configured on this FortiGate unit - CLI:

```
# diag fortitoken info
FORTITOKEN DRIFT STATUS
FTK2000BHV1KRZCC 0 token already activated, and seed won't be returned
FTK2001C5YCRRVEE 0 token already activated, and seed won't be returned
FTKMOB4B94972FBA 0 provisioned
FTKMOB4BA4BE9B84 0 new
Total activated token: 0
Total global activated token: 0
Token server status: reachable
```

This command lists the serial number and drift for each FortiToken configured on this FortiGate unit. This command is useful to check if it is necessary to synchronize the FortiGate and any particular FortiTokens.

Monitoring users

To monitor user activity in the web-based manager, go to **User & Device > Monitor > Firewall**. The list of users who are logged on is displayed with some information about them such as their user group, security policy ID, how long they have been logged on, their IP address, traffic volume, and their authentication method as one of FSSO, NTLM, or firewall (FW-auth).

From this screen you can de-authenticate all users who are logged on. The de-authenticate button is at the top left of this screen.

To see information about banned users go to **User & Device > Monitor > Banned User**. Displayed information about users who have been banned includes what application the triggered the ban (Application Protocol), the reason for the ban (Cause or rule), Created, and when the ban expires.

Filtering the list of users

When there are many users logged on, it can be difficult to locate a specific user or multiple users to analyze. Applying filters to the list allows you to organize the user list to meet your needs, or only display some the users that meet your current requirements.

Select settings bottom at the top right of the screen to adjust columns that are displayed for users, including what order they are displayed in. This can be very helpful in locating information you are looking for.

Each column heading has a grey filter icon. Click on the filter icon to configure a filter for the data displayed in that column. Each column has similar options including a field to enter the filtering information, a check box to select the negative of the text in the field, and the options to add more fields, apply the filter, clear all filters, or cancel without saving. To enter multiple terms in the field, separate each of them with a comma. To filter entries that contain a specific prefix, use an * (asterisk).

For example, to create a filter to display only users with an IP address of `10.11.101.x` who authenticated using one of security policies five through eight, and who belong to the user group `Accounting`.

1. Go to **User & Device > Monitor > Firewall**.
2. Select the filter icon beside **IP address**.
3. Enter `10.11.101.` . and select **Apply**.
4. Select the filter icon beside **Policy ID.**
5. Enter `5-8` and select **Apply**.
6. Select the filter icon beside **User Group.**
7. Enter `Accounting` and select **Apply**.

User groups

A user group is a list of user identities. An identity can be:

- a local user account (username/password stored on the FortiGate unit
- a remote user account (password stored on a RADIUS, LDAP, or TACACS+ server)
- a PKI user account with digital client authentication certificate stored on the FortiGate unit

- a RADIUS, LDAP, or TACACS+ server, optionally specifying particular user groups on that server
- a user group defined on an FSSO server.

Security policies and some types of VPN configurations allow access to specified user groups only. This restricted access enforces Role Based Access Control (RBAC) to your organization's network and its resources. Users must be in a group and that group must be part of the security policy.

In most cases, the FortiGate unit authenticates users by requesting their username and password. The FortiGate unit checks local user accounts first. If a match is not found, the FortiGate unit checks the RADIUS, LDAP, or TACACS+ servers that belong to the user group. Authentication succeeds when a matching username and password are found. If the user belongs to multiple groups on a server, those groups will be matched as well.

FortiOS does not allow username overlaps between RADIUS, LDAP, or TACACS+ servers.

There are four types of FortiGate user groups: Firewall, Fortinet Single Sign-On (FSSO), Guest, and RADIUS Single Sign-On (RSSO) user groups.

Firewall user groups

Firewall user groups are used locally as part of authentication. When a security policy allows access only to specified user groups, users must authenticate. If the user authenticates successfully and is a member of one of the permitted groups, the session is allowed to proceed.

This section includes:

- SSL VPN access
- IPsec VPN access
- Configuring a firewall user group
- Multiple group enforcement support
- User group timeouts

SSL VPN access

SSL VPN settings include a list of the firewall user groups that can access the SSL VPN and the SSL VPN portal that each group will use. When the user connects to the FortiGate unit via HTTPS on the SSL VPN port (default 10443), the FortiGate unit requests a username and password.

SSL VPN access also requires a security policy where the destination is the SSL interface. For more information, see the FortiOS Handbook SSL VPN guide.

IPsec VPN access

A firewall user group can provide access for dialup users of an IPsec VPN. In this case, the IPsec VPN phase 1 configuration uses the **Accept peer ID in dialup group** peer option. The user's VPN client is configured with the username as peer ID and the password as pre-shared key. The user can connect successfully to the IPsec VPN only if the username is a member of the allowed user group and the password matches the one stored on the FortiGate unit.

A user group cannot be used as a dialup group if any member of the group is authenticated using an external authentication server.

For more information, see the FortiOS Handbook IPsec VPN guide.

Configuring a firewall user group

A user group can contain:

- local users, whether authenticated by the FortiGate unit or an authentication server
- PKI users
- authentication servers, optionally specifying particular user groups on the server

To create a Firewall user group - web-based manager:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter a name for the user group.
3. In **Type**, select **Firewall**.
4. Add user names to to the **Members** list.
5. Add authentication servers to the **Remote groups** list.
   By default all user accounts on the authentication server are members of this FortiGate user group. To include only specific user groups from the authentication server, deselect **Any** and enter the group name in the appropriate format for the type of server. For example, an LDAP server requires LDAP format, such as: cn=users,dn=office,dn=example,dn=com
   Remote servers must already be configured in **User & Device > Authentication**.
6. Select **OK**.

To create a firewall user group - CLI example:

In this example, the members of `accounting_group` are `User1` and all of the members of `rad_accounting_group` on `myRADIUS` external RADIUS server.

```
config user group
   edit accounting_group
      set group-type firewall
      set member User1 myRADIUS
      config match
         edit 0
            set server-name myRADIUS
            set group-name rad_accounting_group
         end
      end
```

Matching user group names from an external authentication server might not work if the list of group memberships for the user is longer than 8000 bytes. Group names beyond this limit are ignored.

`server_name` is the name of the RADIUS, LDAP, or TACACS+ server, but it must be a member of this group first and must also be a configured remote server on the FortiGate unit.

`group_name` is the name of the group on the RADIUS, LDAP, or TACACS+ server such as “engineering” or “cn=users,dc=test,dc=com”.

Before using group matching with TACACS+, you must first enable authentication. For example if you have a configured TACACS+ server called myTACS, use the following CLI commands.

```
config user tacacs+
   edit myTACS
   set authorization enable
   next
end
```

For more information about user group CLI commands, see the Fortinet CLI Guide.

Multiple group enforcement support

Previously, when a user belonged to multiple user groups, this user could only access the group services that were within one group. With multiple group enforcement, a user can access the services within the groups that the user is part of.

For example, `userA` belongs to `user_group1`, `user_group2`, `user_group3`, and `user_group4`; previously `userA` could only access services within one of those four groups, typically the group that matches the first security policy. This can be annoying if HTTP access is in `user_group1`, FTP access is in `user_group2`, and email access is in `user_group3`. Now `userA` can access services within `user_group1`, `user_group2`, `user_group3`, and `user_group4`.

This feature is available only in the CLI and is enabled by default. It applies to RADIUS, LDAP, and TACACS+ servers. The new command for this feature is `auth-multi-group` found in `config user settings` and checks all groups a user belongs to for authentication.

User group timeouts

User groups can have timeout values per group in addition to FortiGate-wide timeouts. There are essentially three different types of timeouts that are configurable for user authentication on the FortiGate unit — idle timeout, hard timeout, and session timeout. These are in addition to any external timeouts such as those associated with RADIUS servers.

If VDOMs are enabled, the global level user setting `authtimeout` is the default all VDOMs inherit. If VDOMs are not enabled, user settings authtimeout is the default. The default timeout value is used when the `authtimeout` keyword for a user group is set to zero.

Each type of timeout will be demonstrated using the existing user group `example_group`. Timeout units are minutes. A value of zero indicates the global timeout is used.

Membership in multiple groups

When a user belongs to multiple groups in RADIUS groups, the group auth-timeout values are ignored. Instead the global timeout value is used. The default value is 5 minutes, but it can be set from 1 to 1440 minutes (24 hours).

```
config user setting
   set auth-timeout-type idle-timeout
   set auth-timeout 300
```

```
end
```

Idle timeout

The default type of timeout is idle timeout. When a user initiates a session, it starts a timer. As long as data is transferred in this session, the timer continually resets. If data flow stops, the timer is allowed to advance until it reaches its limit. At that time the user has been idle for too long, and the user is forced to re-authenticate before traffic is allowed to continue in that session.

To configure user group authentication idle timeout - CLI:

```
config user settings
   set auth-timeout-type idle-timeout
end
config user group
   edit example_group
      set authtimeout 5 //range is 0-1440 minutes (0 = use global authtimeout value)
   next
end
```

Hard timeout

Where the idle timeout is reset with traffic, the hard timeout is absolute. From the time the first session a user establishes starts, the hard timeout counter starts. When the timeout is reached, all the sessions for that user must be re-authenticated. This timeout is not affected by any event.

To configure user group authentication hard timeout - CLI:

```
config user settings
   set auth-timeout-type hard-timeout
end
config user group
   edit example_group
      set authtimeout 1440 //range is 0-1440 minutes (0 = use global authtimeout value)
   next
end
```

Session timeout

The session timeout works much like the hard timeout in that its an absolute timer that can not be affected by events. However, when the timeout is reached existing sessions may continue but new sessions are not allowed until re-authentication takes place.

To configure a user group authentication new session hard timeout - CLI:

```
config user setting
   set auth-timeout-type new-session
end

config user group
   edit example_group
      set authtimeout 30 //range is 0-1440 minutes (0 = use global authtimeout value)
   next
end
```

SSO user groups

SSO user groups are part of FSSO authentication and contain only Windows or Novell network users. No other user types are permitted as members. Information about the Windows or Novell user groups and the logon activities of their members is provided by the Fortinet Single Sign On (FSSO) which is installed on the network domain controllers.

You can specify FSSO user groups in security policies in the same way as you specify firewall user groups. FSSO user groups cannot have SSL VPN or dialup IPsec VPN access.

For information about configuring FSSO user groups, see Creating Fortinet Single Sign-On (FSSO) user groups on page 162. For complete information about installing and configuring FSSO, see Agent-based FSSO on page 126.

Configuring Peer user groups

Peer user groups can only be configured using the CLI. Peers are digital certificate holders defined using the `config user peer` command. The peer groups you define here are used in dialup IPsec VPN configurations that accept RSA certificate authentication from members of a peer certificate group.

To create a peer group - CLI example:

```
config user peergrp
   edit vpn_peergrp1
      set member pki_user1 pki_user2 pki_user3
   end
```

Viewing, editing and deleting user groups

To view the list of FortiGate user groups, go to **User & Device > User > User Groups**.

Editing a user group

When editing a user group in the CLI you must set the type of group this will be — either a firewall group, a Fortinet Single Sign-On Service group (FSSO), a Radius based Single Sign-On Service group (RSSO), or a guest group. Once the type of group is set, and members are added you cannot change the group type without removing the members.

In the web-based manager, if you change the type of the group any members will be removed automatically.

To edit a user group - web-based manager:

1. Go to **User & Device > User > User Groups**.
2. Select the user group that you want to edit.
3. Select the **Edit** button.
4. Modify the user group as needed.
5. Select **OK**.

To edit a user group - CLI example:

This example adds user3 to Group1. Note that you must re-specify the full list of users:

```
config user group
   edit Group1
   set group-type firewall
      set member user2 user4 user3
   end
```

Deleting a user group

Before you delete a user group, you must ensure there are no objects referring to, it such as security policies. If there are, you must remove those references before you are able to delete the user group.

To remove a user group - web-based manager:

1. Go to **User & Device > User > User Groups**.
2. Select the user group that you want to remove.
3. Select the **Delete** button.
4. Select **OK**.

To remove a user group - CLI example:

```
config user group
   delete Group2
end
```

Managing Guest Access

Visitors to your premises might need user accounts on your network for the duration of their stay. If you are hosting a large event such as a conference, you might need to create many such temporary accounts. The FortiOS Guest Management feature is designed for this purpose.

A guest user account User ID can be the user's email address, a randomly generated string, or an ID that the administrator assigns. Similarly, the password can be administrator-assigned or randomly generated.

You can create many guest accounts at once using randomly-generated User IDs and passwords. This reduces administrator workload for large events.

User's view of guest access

1. The user receives an email, SMS message, or printout from a FortiOS administrator listing a User ID and password.
2. The user logs onto the network with the provided credentials.
3. After the expiry time, the credentials are no longer valid.

Administrator's view of guest access

1. Create one or more guest user groups.
   All members of the group have the same characteristics: type of User ID, type of password, information fields used, type and time of expiry.
2. Create guest accounts using Guest Management.
3. Use captive portal authentication and select the appropriate guest group.

Configuring guest user access

To set up guest user access, you need to create at least one guest user group and add guest user accounts. Optionally, you can create a guest management administrator whose only function is the creation of guest accounts in specific guest user groups. Otherwise, any administrator can do guest management.

Creating guest management administrators

To create a guest management administrator

1. Go to **System > Admin > Administrators** and create a regular administrator account.
   For detailed information see the System Administration chapter.
2. Select **Restrict to Provision Guest Accounts**.
3. In **Guest Groups**, add the guest groups that this administrator manages.

Creating guest user groups

The guest group configuration determines the fields that are provided when you create a guest user account.

To create a guest user group:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter the following information:

Name	Enter a name for the group.
Type	Guest
Enable Batch Account Creation	Create multiple accounts automatically. When this is enabled: • **User ID** and **Password** are set to **Auto-Generate**. • The user accounts have only **User ID, Password**, and **Expiration** fields. Only the **Expiration** field is editable. If the expiry time is a duration, such as “8 hours”, this is the time after first login. • You can print the account information. Users do not receive email or SMS notification. See To create multiple guest user accounts automatically on page 68.
User ID	Select one of: • Email — User’s email address • Specify — Administrator assigns user ID • Auto-Generate — FortiGate unit creates a random user ID
Password	Select one of: • Specify — Administrator assigns user ID • Auto-Generate — FortiGate unit creates a random password • Disable — no password
Expire Type	Choose one of: • Immediately — expiry time is counted from creation of account • After first login — expiry time is counted from user’s first login
Default Expire Time	Set the expire time. The administrator can change this for individual users.
Enable Name	If enabled, user must provide a name.
Enable Sponsor	If enabled, user form has Sponsor field. Select **Required** if required.
Enable Company	If enabled, user form has Company field. Select **Required**if required.
Enable Email	If enabled, user is notified by email.
Enable SMS	If enabled, user is notified by SMS. Select whether FortiGuard Messaging Service or a another SMS provider is used. You can add SMS providers in **System > Config > Messaging Servers**.

Creating guest user accounts

Guest user accounts are not the same as local user accounts created in **User & Device > User > User Definition**. Guest accounts are not permanent; they expire after a defined time period. You create guest accounts in **User & Device > User > Guest Management**.

To create a guest user account

1. Go to **User & Device > User > Guest Management.**
2. In **Guest Groups**, select the guest group to manage.
3. Select **Create New** and fill in the fields in the **New User** form.
   Fields marked Optional can be left blank. The guest group configuration determines the fields that are available.
4. Select **OK**.

To create multiple guest user accounts automatically

1. Go to **User & Device > User > Guest Management.**
2. In **Guest Groups**, select the guest group to manage.
   The guest group must have the **Enable Batch Guest Account Creation** option enabled.
3. Select **Create New > Multiple Users**.
   Use the down-pointing caret to the right of **Create New**.
4. Enter **Number of Accounts**.
5. Optionally, change the **Expiration**.
6. Select **OK**.

Guest Management Account List

Go to **User & Device > User > Guest Management** to create, view, edit or delete guest user accounts.

Create New	Creates a new guest user account.
Edit	Edit the selected guest user account.
Delete	Delete the selected guest user account.
Purge	Remove all expired accounts from the list.
Send	Send the user account information to a printer or to the guest. Depending on the group settings and user information, the information can be sent to the user by email or SMS.
Refresh	Update the list.
Guest Groups	Select the guest group to list. New accounts are added to this group.
User ID	The user ID. Depending on the guest group settings, this can be the user's email address, an ID that the administrator specified, or a randomly-generated ID.

Expires	Indicates a duration such as “3 hours”. A duration on its own is relative to the present time. Or, the duration is listed as “after first login.”

Guest access in a retail environment

Some retail businesses such as coffee shops provide free Wi-Fi Internet access for their customers. For this type of application, the FortiOS guest management feature is not required; the Wi-Fi access point is open and customers do not need logon credentials. However, the business might want to contact its customers later with promotional offers to encourage further patronage. Using an Email Collection portal, it is possible to collect customer email addresses for this purpose. The security policy grants network access only to users who provide a valid email address.

The first time a customer’s device attempts to use the Wi-Fi connection, FortiOS requests an email address, which it validates. The customer’s subsequent connections go directly to the Internet without interruption.

Creating an email harvesting portal

The customer’s first contact with your network will be with a captive portal which presents a web page requesting an email address. When FortiOS has validated the email address, the customer’s device MAC address is added to the Collected Emails device group.

To create the email collection portal:

1. Go to **WiFi & Switch Controller > WiFi Network > SSID** and edit your SSID.
2. Set **Security Mode** to **Captive Portal**.
3. Set **Portal Type** to **Email Collection**.
4. Optionally, in **Customize Portal Messages** select **Email Collection.**

You can change the portal content and appearance. See Customizing captive portal pages on page 89.

To create the email collection portal - CLI:

In this example the `freewifi` Wi-Fi interface is modified to present an email collection captive portal.

```
config wireless-controller vap
   edit freewifi
      set security captive-portal
      set portal-type email-collect
end
```

Creating the security policy

You need configure a security policy that allows traffic to flow from the Wi-Fi SSID to the Internet interface but only for members of the Collected Emails device group. This policy must be listed first. Unknown devices are not members of the Collected Emails device group, so they do not match the policy.

To create the security policy:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information:

Incoming Interface	freewifi
Source Address	all
Source Device Type	Collected Emails
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
NAT	On

3. Select **OK**.

To create the authentication rule - CLI:

```
config firewall policy
   edit 3
      set srcintf "freewifi"
      set dstintf "wan1"
      set srcaddr "all"
      set action accept
      set devices collected-emails
      set nat enable
      set schedule "always"
      set service "ALL"
   end
```

Checking for harvested emails

In the web-based manager, go to **User & device > Device > Device Definitions**. In the CLI you can use the `diagnose user device list` command. For example,

```
FGT-100D # diagnose user device list
hosts
   vd 0 d8:d1:cb:ab:61:0f gen 35 req 30 redir 1 last 43634s 7-11_2-int
      ip 10.0.2.101 ip6 fe80::dad1:cbff:feab:610f
      type 2 'iPhone' src http c 1 gen 29
      os 'iPhone' version 'iOS 6.0.1' src http id 358 c 1
      email 'yo@yourdomain.com'
   vd 0 74:e1:b6:dd:69:f9 gen 36 req 20 redir 0 last 39369s 7-11_2-int
      ip 10.0.2.100 ip6 fe80::76e1:b6ff:fedd:69f9
      type 1 'iPad' src http c 1 gen 5
      os 'iPad' version 'iOS 6.0' src http id 293 c 1
      host 'Joes's-iPad' src dhcp
      email 'you@fortinet.com'
```

Configuring authenticated access

When you have configured authentication servers, users, and user groups, you are ready to configure security policies and certain types of VPNs to require user authentication.

This section describes:

Authentication timeout

An important feature of the security provided by authentication is that it is temporary—a user must re-authenticate after logging out. Also if a user is logged on and authenticated for an extended period of time, it is a good policy to have them re-authenticate at set periods. This ensures a user's session is cannot be spoofed and used maliciously for extended periods of time — re-authentication will cut any spoof attempts short. Shorter timeout values are more secure.

Security authentication timeout

You set the security user authentication timeout to control how long an authenticated connection can be idle before the user must authenticate again. The maximum timeout is 1440 minutes (24 hours).

To set the security authentication timeout - web-based manager:

1. Go to **User & Device > Authentication > Settings**.
2. Enter the **Authentication Timeout** value in minutes.
   The default authentication timeout is 5 minutes.
3. Select **Apply**.

SSL VPN authentication timeout

You set the SSL VPN user authentication timeout (**Idle Timeout**) to control how long an authenticated connection can be idle before the user must authenticate again. The maximum timeout is 259 200 seconds. The default timeout is 300 seconds.

To set the SSL VPN authentication timeout - web-based manager:

1. Go to **VPN > SSL > Settings**.
2. Under **Idle Logout**, make sure that **Logout users when inactive for specified period** is enabled and enter

the **Inactive For** value (seconds).

3. Select **Apply**.

Password policy

Password authentication is effective only if the password is sufficiently strong and is changed periodically. By default, the FortiGate unit requires only that passwords be at least eight characters in length. You can set a password policy to enforce higher standards for both length and complexity of passwords. Password policies can apply to administrator passwords or IPsec VPN preshared keys.

To set a password policy in the web-based manager, go to **System > Admin > Settings**. In the CLI, use the `config system password-policy` command.

The default minimum password length on the FortiGate unit is eight characters, but up to 128 characters is permitted.

Users usually create passwords composed of alphabetic characters and perhaps some numbers. Password policy can require the inclusion of uppercase letters, lowercase letters, numerals or punctuation characters.

Configuring password minimum requirement policy

Best practices dictate that passwords include:

- one or more uppercase characters
- one or more lower case characters
- one or more of the numerals
- one or more special characters.

The minimum number of each of these types of characters can be set in both the web-based manager and the CLI.

The following procedures show how to force administrator passwords to contain at least two uppercase, four lower care, two digits, and one special character. Leave the minimum length at the default of eight characters.

To change administrator password minimum requirements - web-based manager:

1. Go to **System > Admin > Settings**.
2. Select **Enable Password Policy**.
3. Select **Must Contain at Least**.
4. Enter the following information:

Upper Case Letters	2
Lower Case Letters	4
Numbers	2
Special Characters	1

5. Under **Apply Password Policy to**, select **Administrator Password**.
6. Select **Apply**.

To change administrator password minimum requirements - CLI:

```
config system password-policy
   set status enable
   set apply-to admin-password
   set min-upper-case-letter 2
   set min-lower-case-letter 4
   set min-number 2
   set min-non-alphanumeric 1
   set change-4-characters enable
end
```

The `change-4-characters` option forces new passwords to change a minimum of four characters in the old password. Changing fewer characters results in the new password being rejected. This option is only available in the CLI.

Password best practices

In addition to length and complexity, there are security factors that cannot be enforced in a policy. Guidelines issued to users will encourage proper password habits.

Best practices dictate that password expiration also be enabled. This forces passwords to be changed on a regular basis. You can set the interval in days. The more sensitive the information this account has access to, the shorter the password expiration interval should be. For example 180 days for guest accounts, 90 days for users, and 60 days for administrators.

Avoid:

- real words found in any language dictionary
- numeric sequences, such as “12345”
- sequences of adjacent keyboard characters, such as “qwerty”
- adding numbers on the end of a word, such as “hello39”
- adding characters to the end of the old password, such as “hello39” to “hello3900”
- repeated characters
- personal information, such as your name, birthday, or telephone number.

Maximum logon attempts and blackout period

When you logon and fail to enter the correct password you could be a valid user, or a hacker attempting to gain access. For this reason, best practices dictate to limit the number of failed attempts to logon before a blackout period where you cannot logon.

To set a maximum of five failed authentication attempts before the blackout, using the following CLI command:

```
config user setting
   set auth-invalid-max 5
end
```

To set the length of the blackout period to five minutes, or 300 seconds, once the maximum number of failed logon attempts has been reached, use the following CLI command:

```
config user setting
   set auth-blackout-time 300
```

```
end
```

Authentication protocols

When user authentication is enabled on a security policy, the authentication challenge is normally issued for any of the four protocols, HTTP, HTTPS, FTP, and Telnet, which are dependent on the connection protocol. By making selections in the Protocol Support list, the user controls which protocols support the authentication challenge. The user must connect with a supported protocol first, so that they can subsequently connect with other protocols.

For example, if you have selected HTTP, FTP, or Telnet, a username and password-based authentication occurs. The FortiGate unit then prompts network users to input their security username and password. If you have selected HTTPS, certificate-based authentication (HTTPS, or HTTP redirected to HTTPS only) occurs.

FTP and Telnet authentication replacement messages cannot be customized. For HTTP and HTTPS replacement messages see Authentication replacement messages on page 76.

For certificate-based authentication, you must install customized certificates on the FortiGate unit and on the browsers of network users. If you do not install certificates on the network user's web browser, the network users may see an SSL certificate warning message and have to manually accept the default FortiGate certificate. The network user's web browser may deem the default certificate as invalid.

When you use certificate authentication, if you do not specify any certificate when you create the security policy, the global settings are used. If you specify a certificate, the per-policy setting will overwrite the global setting. For more information about the use of certification authentication see Certificate-based authentication on page 95.

To set the authentication protocols

1. Go to **User & Device > Authentication > Settings**.
2. In **Protocol Support**, select the required authentication protocols.
3. If using HTTPS protocol support, in **Certificate**, select a Local certificate from the drop-down list.
4. Select **Apply**.

Authentication in Captive Portals

Network interfaces, including WiFi interfaces, can perform authentication at the interface level using a captive portal — an HTML form that requests the user's name and password. A captive portal is useful where all users connecting to the network interface must authenticate. Optionally, on a WiFi interface, the captive portal can be combined with a terms of service disclaimer to which the user must agree before gaining access. For more information, see Captive portals on page 87.

Once successfully authenticated, the user's session passes to the firewall.

Authentication in security policies

Security policies control traffic between FortiGate interfaces, both physical interfaces and VLAN subinterfaces. The firewall tries to match the session's user or group identity, device type, destination, etcetera to a security policy. When a match is found, the user connects to the requested destination. If no security policy matches, the user is denied access.

A user who has not already been authenticated by a captive portal, FSSO, or RSSO can match only policies where no user or user group is specified. If no such policy exists, the firewall requests authentication. If the user can authenticate and the session can be matched to a policy, the user connects to the requested destination, otherwise, the user is denied access.

This section includes:

Enabling authentication protocols

Users can authenticate using FTP, HTTP, HTTPS, and Telnet. However, these protocols must be enabled first.

Another authentication option is to redirect any attempts to authenticate using HTTP to a more secure channel that uses HTTPS. This forces users to a more secure connection before entering their user credentials.

To enable support for authentication protocols - web-based manager:

1. Go to **User & Device > Authentication > Settings**.
2. Select one or more of HTTP, HTTPS, FTP, Telnet, or Redirect HTTP Challenge to a Secure Channel (HTTPS). Only selected protocols will be available for use in authentication.
3. Select the **Certificate** to use, for example `Fortinet_Factory`.
4. Select **Apply**.

To enable support for authentication protocols - CLI:

```
config user setting
   set auth-type ftp http https telnet
   set auth-cert Fortinet_Factory
end
```

Authentication replacement messages

A replacement message is the body of a webpage containing a message about a blocked website message, a file too large message, a disclaimer, or even a login page for authenticating. The user is presented with this message instead of the blocked content.

Authentication replacement messages are the prompts a user sees during the security authentication process such as login page, disclaimer page, and login success or failure pages. These are different from most replacement messages because they are interactive requiring a user to enter information, instead of simply informing the user of some event as other replacement messages do.

Replacement messages have a system-wide default configuration, a per-VDOM configuration, and disclaimers can be customized for multiple security policies within a VDOM.

These replacement messages are used for authentication using HTTP and HTTPS. Authentication replacement messages are HTML messages. You cannot customize the security authentication messages for FTP and Telnet.

The authentication login page and the authentication disclaimer include replacement tags and controls not found on other replacement messages.

More information about replacement messages can be found in the `config system replacemsg` section of the FortiOS CLI Reference.

List of authentication replacement messages

Replacement message name (CLI name)	Description
Login challenge page (auth-challenge-page)	This HTML page is displayed if security users are required to answer a question to complete authentication. The page displays the question and includes a field in which to type the answer. This feature is supported by RADIUS and uses the generic RADIUS challenge-access auth response. Usually, challenge-access responses contain a Reply-Message attribute that contains a message for the user (for example, “Please enter new PIN”). This message is displayed on the login challenge page. The user enters a response that is sent back to the RADIUS server to be verified. The Login challenge page is most often used with RSA RADIUS server for RSA SecurID authentication. The login challenge appears when the server needs the user to enter a new PIN. You can customize the replacement message to ask the user for a SecurID PIN. This page uses the %%QUESTION%% tag.

Replacement message name (CLI name)	Description
Disclaimer page (auth-disclaimer-page-1) (auth-disclaimer-page-2) (auth-disclaimer-page-3)	This page prompts user to accept the displayed disclaimer when leaving the captive portal to access Internet resources. It is displayed when the captive portal type is **Authentication and Disclaimer** or **Disclaimer Only**. In the CLI, the auth-disclaimer-page-2 and auth-disclaimer-page-3 pages seamlessly extend the size of the disclaimer page from 8 192 characters to 16 384 and 24 576 characters respectively. In the web-based manager this is handled automatically. See Disclaimer on page 79.
Email token page (auth-email-token-page)	The page prompting a user to enter their email token. See Email on page 1.
FortiToken page (auth-fortitoken-page)	The page prompting a user to enter their FortiToken code. See FortiToken on page 53.

Keepalive page
(auth-keepalive-page)
	The HTML page displayed with security authentication keepalive is enabled using the following CLI command:
	
	`config system globalset auth-keepalive enable`
	`end`
	
	Authentication keepalive keeps authenticated firewall sessions from ending when the authentication timeout ends. In the web-based manager, go to **User & Device > Authentication > Settings** to set the **Authentication Timeout**.
	
	This page includes %%TIMEOUT%%.

Login failed page (auth-login-failed-page)	The Disclaimer page replacement message does not re-direct the user to a redirect URL or the security policy does not include a redirect URL. When a user selects the button on the disclaimer page to decline access through the FortiGate unit, the Declined disclaimer page is displayed.
Login page (auth-login-page)	The authentication HTML page displayed when users who are required to authenticate connect through the FortiGate unit using HTTP or HTTPS. Prompts the user for their username and password to login. This page includes %%USERNAMEID%% and %%PASSWORDID%% tags.
Declined disclaimer page (auth-reject-page)	The page displayed if a user declines the disclaimer page. See Disclaimer on page 79.

Replacement message name (CLI name)	Description
SMS Token page (auth-sms-token-page)	The page prompting a user to enter their SMS token. See SMS on page 52.
Success message (auth-success-msg)	The page displayed when a user successfully authenticates. Prompts user to attempt their connection again (as the first was interrupted for authentication).

Access to the Internet

A policy for accessing the Internet is similar to a policy for accessing a specific network, but the destination address is set to **all**. The destination interface is the one that connects to the Internet Service Provider (ISP). For general purpose Internet access, the Service is set to ALL.

Access to HTTP, HTTPS, FTP and Telnet sites may require access to a domain name service. DNS requests do not trigger authentication. You must configure a policy to permit unauthenticated access to the appropriate DNS server, and this policy must **precede** the policy for Internet access. Failure to do this will result in the lack of a DNS connection and a corresponding lack of access to the Internet.

Configuring authentication security policies

To include authentication in a security policy, the policy must specify user groups. A security policy can authenticate by certificate, FSSO, and NTLM. The two exceptions to this are RADIUS SSO and FSSO Agents. See SSO using RADIUS accounting records on page 170, and Introduction to FSSO agents on page 127.

Before creating a security policy, you need to configure one or more users or user groups. For more information, see Users and user groups on page 46.

Creating the security policy is the same as a regular security policy except you must select the action specific to your authentication method:

Authentication methods allowed for each policy Action

Action	Authentication method	Where authentication is used
ACCEPT	FSSO Agent or a security policy that specifies an FSSO user group	Agent-based FSSO on page 126.
	NTLM	See NTLM authentication on page 80.
	Certificates	See Configuring certificate-based authentication on page 107.
	RADIUS SSO	See SSO using RADIUS accounting records on page 170.
DENY	none	none

Disclaimer

A WiFi or SSL captive portal can include a disclaimer message presented after the user authenticates. The user must agree to the terms of the disclaimer to access network resources.

Customizing authentication replacement messages

Customizing disclaimers or other authentication replacement messages involves changing the text of the disclaimer message, and possibly the overall appearance of the message.

Changing the disclaimer in **System > Config > Replacement messages** is not the same as selecting to customize a disclaimer used in a captive portal. The **System > Config** location is the default message that all disclaimers inherit. The captive portal location is a customized disclaimer that inherits the default format for the disclaimer message, but then can be customized for this portal.

To customize the disclaimer for a captive portal - web-based manager:

1. Go to **System > Network > Interface**. Either select an existing interface or create a new one.
2. Under **Security Mode**, select **Captive Portal**, and enable **Customize Portal Messages**.
3. Select the **Edit** icon. You can select and edit any of the pages. Change your text or layout as needed.

Enabling security logging

There are two types of logging that relate to authentication — event logging, and security logging.

When enabled, event logging records system events such as configuration changes, and authentication. To configure event logging, go to **Log&Report > Log Config > Log Settings** and enable **Event Logging**. Select the events you want to log, such as **User activity event**.

When enabled, security logging will log security profile and security policy traffic.

You must enable logging within a security policy, as well as the options that are applied to a security policy, such as security profiles features. Event logs are enabled within the Event Log page.

For more information on logging, see the FortiOS Log and Reporting guide.

For more information on specific types of log messages, see the FortiOS Log Message Reference.

You need to set the logging severity level to **Notification** when configuring a logging location to record traffic log messages.

To enable logging within an existing security policy - web-based manager:

1. Go to **Policy & Objects > Policy > IPv4**.
2. Expand to reveal the policy list of a policy.
3. Select the security policy you want to enable logging on and then select **Edit**.
4. To log all general firewall traffic, select the check box beside **Log Allowed Traffic**, and choose to enable **Security Events** or **All Sessions**.
5. Select **OK**.

Identity-based policy

An identity-based policy (IBP) performs user authentication in addition to the normal security policy duties. If the user does not authenticate, access to network resources is refused. This enforces Role Based Access Control (RBAC) to your organization's network and resources.

Identity-based policies also support Single Sign-On operation. The user groups selected in the policy are of the Fortinet Single Sign-On (FSSO) type.

User authentication can occur through any of the following supported protocols, including: HTTP, HTTPS, FTP, and Telnet. The authentication style depends on which of these protocols is included in the selected security services group and which of those enabled protocols the network user applies to trigger the authentication challenge.

For username and password-based authentication (HTTP, FTP, and Telnet) the FortiGate unit prompts network users to enter their username, password, and token code if two-factor authentication is selected for that user account. For certificate-based authentication, including HTTPS or HTTP redirected to HTTPS only, see Certificate authentication on page 81.

With identity-based policies, the FortiGate unit allows traffic that matches the source and destination addresses, device types, and so on. This means specific security policies must be placed **before** more general ones to be effective.

When the identity-based policy has been configured, the option to customize authentication messages is available. This allows you to change the text, style, layout, and graphics of the replacement messages associated with this firewall policy. When enabled, customizing these messages follows the same method as changing the disclaimer. See Disclaimer on page 79.

Types of authentication also available in identity-based policies are

- NTLM authentication
- Certificate authentication

NTLM authentication

NT LAN Manager (NTLM) protocol can be used as a fallback for authentication when the Active Directory (AD) domain controller is unreachable. NTLM uses the web browser to send and receive authentication information. See "NTLM" and "FSSO NTLM authentication support".

To enable NTLM

1. Edit the policy in the CLI to enable NTLM. For example, if the policy ID is 4:
2. Go to **Policy & Objects > Policy > IPv4** and note the **ID** number of your FSSO policy.
3. The policy must have an FSSO user group as **Source User(s)**. There must be at least one FSSO Collector agent configured on the FortiGate unit.

```
config firewall policy
  edit 4
    set ntlm enable
  end
```

NTLM guest access

Guest profile access may be granted to users who fail NTLM authentication, such as visitors who have no user credentials on the network. To allow guest user access, edit the FSSO security policy in the CLI, like this:

```
config firewall policy
   edit 4
      set ntlm enable
      set ntlm-guest enable
   end
```

NTLM enabled browsers - CLI

User agent strings for NTLM enabled browsers allow the inspection of initial HTTP-User-Agent values, so that non-supported browsers are able to go straight to guest access without needlessly prompting the user for credentials that will fail. `ntlm-guest` must be enabled to use this option.

```
config firewall policy
   edit 4
      set ntlm enable
      set ntlm-guest enable
      set ntlm-enabled-browsers <user_agent_string>
   next
   end
```

`<user_agent_string>` is the name of the browser that is NTLM enabled. Examples of these values include “MSIE”, “Mozilla” (which includes FireFox), and “Opera”.

Value strings can be up to 63 characters in length, and may not contain cross site scripting (XSS) vulnerability characters such as brackets. The FortiGate unit prevents use of these characters to prevent exploit of cross site scripting (XSS) vulnerabilities.

Certificate authentication

You can configure certificate-based authentication for FortiGate administrators, SSL VPN users, and IPsec VPN users. See Configuring certificate-based authentication on page 107.

Certificates are also inherent to the HTTPS protocol, where the browser validates the server’s identity using certificates. A site certificate must be installed on the FortiGate unit and the corresponding Certificate Authority (CA) certificate installed in the web browser.

To force the use of HTTPS, go to **User & Device > Authentication > Settings** and select **Redirect HTTP Challenge to a Secure Channel (HTTPS)**.

Restricting number of concurrent user logons

Some users on your network may often have multiple account sessions open at one time either to the same network resource or accessing to the admin interface on the FortiGate unit.

While there are valid reasons for having multiple concurrent sessions open, hackers also do this to speed up their malicious work. Often a hacker is making multiple attempts to gain access to the internal network or the admin interface of the FortiGate unit, usually from different IP addresses to appear to the FortiGate unit as legitimate users. For this reason, the more concurrent sessions a hacker has open at once, the faster they will achieve their goal.

To help prevent this, you can disallow concurrent administrative access using the same administrator user name, but from a different IP address. This allows valid users to continue their legitimate work while limiting hackers' activity.

To disable concurrent administrator sessions - CLI:

```
config system global
   set admin-concurrent disable
end
```

VPN authentication

All VPN configurations require users to authenticate. Authentication based on user groups applies to:

- SSL VPNs
- PPTP and L2TP VPNs
- an IPsec VPN that authenticates users using dialup groups
- a dialup IPsec VPN that uses XAUTH authentication (Phase 1)

You must create user accounts and user groups before performing the procedures in this section. If you create a user group for dialup IPsec clients or peers that have unique peer IDs, their user accounts must be stored locally on the FortiGate unit. You cannot authenticate these types of users using a RADIUS or LDAP server.

Configuring authentication of SSL VPN users

The general procedure for authenticating SSL VPN users is:

1. Configure user accounts.
2. Create one or more user groups for SSL VPN users.
3. Enable SSL VPN.
4. Optionally, set inactivity and authentication timeouts.
5. Configure a security policy with the user groups you created for SSL VPN users.
   See FortiOS Handbook SSL VPN guide.

Configuring authentication timeout

By default, the SSL VPN authentication expires after 8 hours (28 800 seconds). You can change it only in the CLI, and the time entered must be in seconds. The maximum time is 72 hours (259 200 seconds). For example, to change this timeout to one hour, you would enter:

```
config vpn ssl settings
   set auth-timeout 3600
end
```

If you set the authentication timeout (`auth-timeout`) to 0 when you configure the timeout settings, the remote client does not have to re-authenticate unless they log out of the system. To fully take advantage of this setting, the value for `idle-timeout` has to be set to 0 also, so that the client does not time out if the maximum idle time is reached. If the `idle-timeout` is not set to the infinite value, the system will log out if it reaches the limit set, regardless of the `auth-timeout` setting.

Configuring authentication of remote IPsec VPN users

An IPsec VPN on a FortiGate unit can authenticate remote users through a dialup group. The user account name is the peer ID and the password is the pre-shared key.

Authentication through user groups is supported for groups containing only local users. To authenticate users using a RADIUS or LDAP server, you must configure XAUTH settings. See Configuring XAuth authentication.

To configure user group authentication for dialup IPsec - web-based manager:

1. Configure the dialup users who are permitted to use this VPN. Create a user group with Type:Firewall and add them to it.
   For more information, see Users and user groups on page 46
2. Go to **VPN > IPsec > Wizard**, select **Dialup**, choose a name for the VPN, and enter the following information.

Incoming Interface	Select the incoming interface name.
Authentication Method	List of authentication methods available for users. Select **Preshared Key** and enter the preshared key.
User Group	Select the user group that is to be allowed access to the VPN. The listed user groups contain only users with passwords on the FortiGate unit.

3. Select **Next** and continue configure other VPN parameters as needed.
4. Select **OK**.

To configure user group authentication for dialup IPsec - CLI example:

The `peertype` and `usrgrp` options configure user group-based authentication.

```
config vpn ipsec phase1
   edit office_vpn
      set interface port1
      set type dynamic
      set psksecret yORRAzltNGhzgtV32jend
      set proposal 3des-sha1 aes128-sha1
      set peertype dialup
      set usrgrp Group1
   end
```

Configuring XAuth authentication

Extended Authentication (XAuth) increases security by requiring additional user authentication information in a separate exchange at the end of the VPN Phase 1 negotiation. The FortiGate unit asks the user for a username and password. It then forwards the user's credentials (the password is encrypted) to an external RADIUS or LDAP server for verification.

XAuth can be used in addition to or in place of IPsec phase 1 peer options to provide access security through an LDAP or RADIUS authentication server. You must configure a dialup user group whose members are all externally authenticated.

To configure authentication for a dialup IPsec VPN - web-based manager:

1. Configure the users who are permitted to use this VPN. Create a user group and add the users to the group. For more information, see "Users and user groups" on page 46.
2. Go to **VPN > IPsec > Wizard**, select **Dialup**, choose a name for the VPN, and enter the following information.

Incoming Interface	Select the incoming interface name.
Authentication Method	List of authentication methods available for users. Select **Preshared Key** and enter the preshared key.
User Group	Select the user group that is to be allowed access to the VPN. The listed user groups contain only users with passwords on the FortiGate unit.

3. Select **Next** and continue configure other VPN parameters as needed.
4. Select **OK**.
5. Go to **VPN > IPsec > Tunnels**, edit the Tunnel just created, select **Convert To Custom Tunnel**, and edit **XAUTH** as following:

Type	Select **PAP**, **CHAP**, or **AUTO**. Use CHAP whenever possible. Use PAP with all implementations of LDAP and with other authentication servers that do not support CHAP, including some implementations of Microsoft RADIUS. Use AUTO with the Fortinet Remote VPN Client and where the authentication server supports CHAP but the XAuth client does not.
User Group	Select the user group that is to have access to the VPN. The list of user groups does not include any group that has members whose password is stored on the FortiGate unit.

6. Select **OK**.

For more information about XAUTH configuration, see the IPsec VPN chapter of the FortiOS Handbook.

To configure authentication for a dialup IPsec VPN - CLI example:

The `xauthtype` and `authusrgrp` fields configure XAuth authentication.

```
config vpn ipsec phase1
   edit office_vpn
      set interface port1
      set type dynamic
      set psksecret yORRAzltNGhzgtV32jend
      set proposal 3des-sha1 aes128-sha1
      set peertype dialup
      set xauthtype pap
      set usrgrp Group1
   end
```

Some parameters specific to setting up the VPN itself are not shown here. For detailed information about configuring IPsec VPNs, see the FortiOS Handbook IPsec VPN guide.

Configuring authentication of PPTP VPN users and user groups

Configuration of a PPTP VPN is possible only through the CLI. You can configure user groups and security policies using either CLI or web-based manager.

LDAP user authentication is supported for PPTP, L2TP, IPsec VPN, and firewall authentication.

However, with PPTP, L2TP, and IPsec VPN, PAP (Packet Authentication Protocol) is supported, while CHAP (Challenge Handshake Authentication Protocol) is not.

To configure authentication for a PPTP VPN

1. Configure the users who are permitted to use this VPN. Create a security user group and add them to it. For more information, see Users and user groups on page 46.
2. Configure the PPTP VPN in the CLI as in this example.

```
config vpn pptp
   set status enable
   set sip 192.168.0.100
   set eip 192.168.0.110
   set usrgrp PPTP_Group
end
```

The `sip` and `eip` fields define a range of virtual IP addresses assigned to PPTP clients.

Configure a security policy. The source interface is the one through which the clients will connect. The source address is the PPTP virtual IP address range. The destination interface and address depend on the network to which the clients will connect. The policy action is ACCEPT.

Configuring authentication of L2TP VPN users/user groups

Configuration of a L2TP VPN is possible only through the CLI. You can configure user groups and security policies using either CLI or web-based manager.

LDAP user authentication is supported for PPTP, L2TP, IPsec VPN, and firewall authentication.

However, with PPTP, L2TP, and IPsec VPN, PAP (Packet Authentication Protocol) is supported, while CHAP (Challenge Handshake Authentication Protocol) is not.

To configure authentication for a L2TP VPN

1. Configure the users who are permitted to use this VPN. Create a user group and add them to it. For more information, see Users and user groups on page 46.
2. Configure the L2TP VPN in the CLI as in this example.

```
config vpn l2tp
   set status enable
   set sip 192.168.0.100
   set eip 192.168.0.110
   set usrgrp L2TP_Group
end
```

The `sip` and `eip` fields define a range of virtual IP addresses assigned to L2TP clients.

3. Configure a security policy. The source interface is the one through which the clients will connect. The source address is the L2TP virtual IP address range. The destination interface and address depend on the network to which the clients will connect. The policy action is ACCEPT.

Captive portals

A captive portal is a convenient way to authenticate web users on wired or WiFi networks.

This section describes:

Introduction to Captive Portals

You can authenticate your users on a web page that requests the user's name and password. Until the user authenticates successfully, the authentication page is returned in response to any HTTP request. This is called a captive portal.

After successful authentication, the user accesses the requested URL and can access other web resources, as permitted by security policies. Optionally, the captive portal itself can allow web access to only the members of specified user group.

The captive portal can be hosted on the FortiGate unit or on an external authentication server. You can configure captive portal authentication on any network interface, including WiFi and VLAN interfaces.

When a captive portal is configured on a WiFi interface, the access point initially appears open. The wireless client can connect to the access point with no security credentials, but sees only the captive portal authentication page.

WiFi captive portal types:

- **Authentication** — until the user enters valid credentials, no communication beyond the AP is permitted.
- **Disclaimer + Authentication** — immediately after successful authentication, the portal presents the disclaimer page—an acceptable use policy or other legal statement—to which the user must agree before proceeding.
- **Disclaimer Only** — the portal presents the disclaimer page—an acceptable use policy or other legal statement—to which the user must agree before proceeding. The authentication page is not presented.
- **Email Collection** — the portal presents a page requesting the user's email address, for the purpose of contacting the person in future. This is often used by businesses who provide free WiFi access to their customers. The authentication page is not presented.

Configuring a captive portal

Captive portals are configured on network interfaces. On a physical (wired) network interface, you edit the interface configuration in **System > Network > Interfaces** and set **Security Mode** to **Captive Portal**. A WiFi interface does not exist until the WiFi SSID is created. You can configure a WiFi captive portal at the time that you create the SSID. Afterwards, the captive portal settings will also be available by editing the WiFi network interface in **System > Network > Interfaces**.

To configure a wired Captive Portal - web-based manager:

1. Go to **System > Network > Interfaces** and edit the interface to which the users connect.
2. In **Security Mode** select **Captive Portal**.

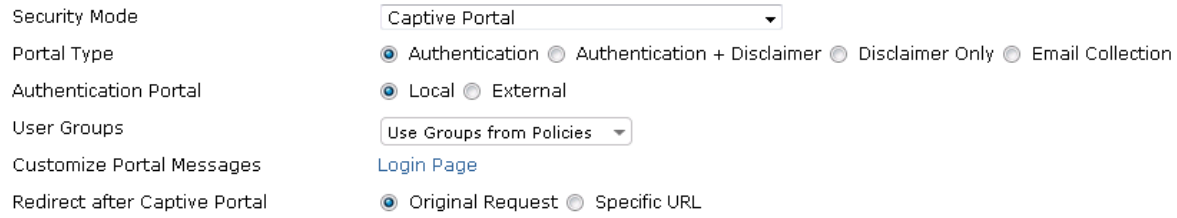
3. Enter

Authentication Portal	Local - portal hosted on the FortiGate unit. Remote - enter FQDN or IP address of external portal.
User Groups	Select permitted user groups or select **Use Groups from Policies**, which permits the groups specified in the security policy. **Use Groups from Policies** is not available in WiFi captive portals.
Exempt List	Select exempt lists whose members will not be subject to captive portal authentication.
Customize Portal Messages	Enable, then select Edit. See Customizing captive portal pages on page 89.

4. Select **OK**.

To configure a WiFi Captive Portal - web-based manager:

1. Go to **WiFi Controller > WiFi Network > SSID** and create your SSID.
   If the SSID already exists, you can edit the SSID or you can edit the WiFi interface in **System > Network > Interfaces**.
2. In **Security Mode**, select **Captive Portal**.



3. Enter

Portal Type	The portal can provide authentication and/or disclaimer, or perform user email address collection. See Introduction to Captive Portals on page 87.
Authentication Portal	Local - portal hosted on the FortiGate unit. Remote - enter FQDN or IP address of external portal.
User Groups	Select permitted user groups.
Exempt List	Select exempt lists whose members will not be subject to captive portal authentication.
Customize Portal Messages	Click the link of the portal page that you want to modify. See "Captive portals" on page 89.

4. Select **OK**.

Exemption from the captive portal

A captive portal requires all users on the interface to authenticate. But some devices are not able to authenticate. You can create an exemption list of these devices. For example, a printer might need to access the Internet for firmware upgrades. Using the CLI, you can create an exemption list to exempt all printers from authentication.

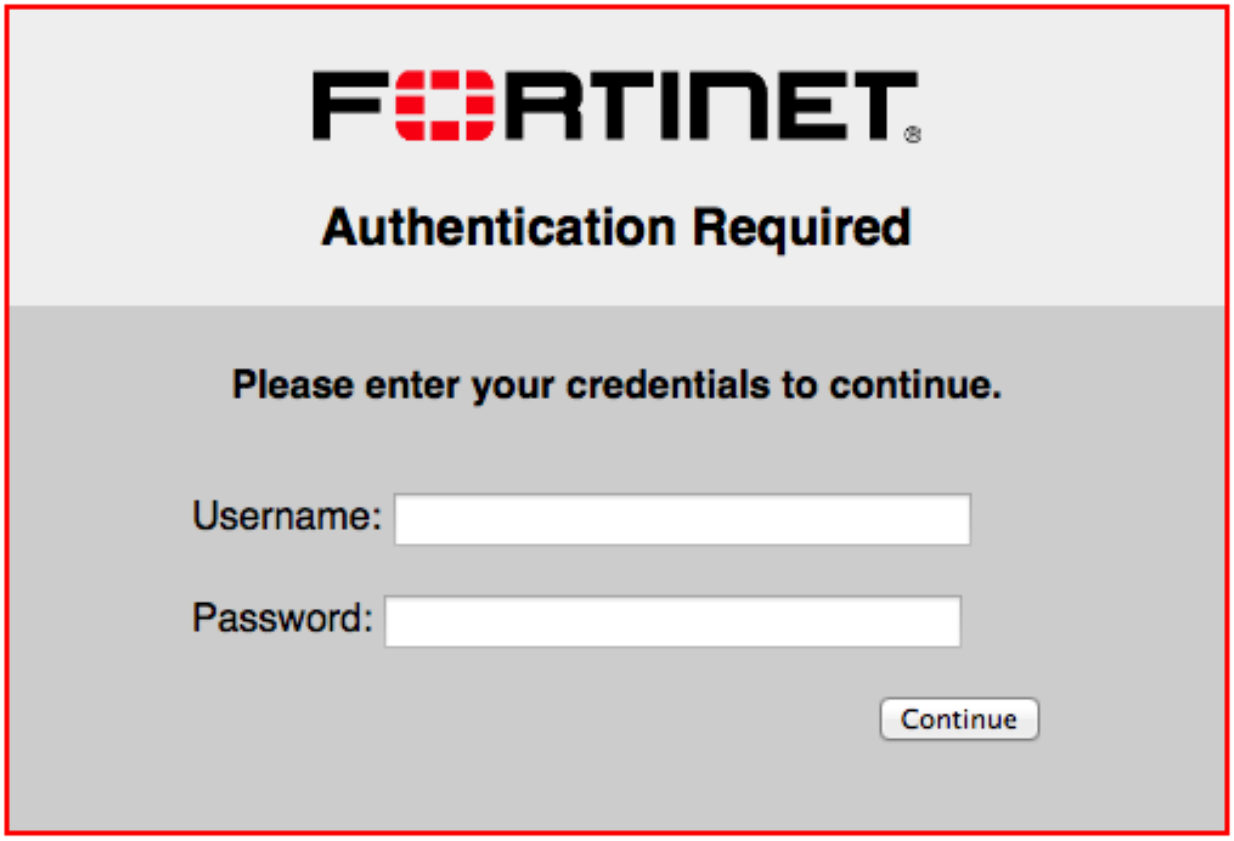
```
config user security-exempt-list
   edit r_exempt
      config rule
         edit 1
            set devices printer
         end
      end
```

Customizing captive portal pages

These pages are defined in replacement messages. Defaults are provided. In the web-based manager, you can modify the default messages in the SSID configuration by selecting **Customize Portal Messages**. Each SSID can have its own unique portal content.

The captive portal contains the following default web pages:

- **Login page**—requests user credentials



Typical modifications for this page would be to change the logo and modify some of the text.

You can change any text that is not part of the HTML code nor a special tag enclosed in double percent (%) characters.

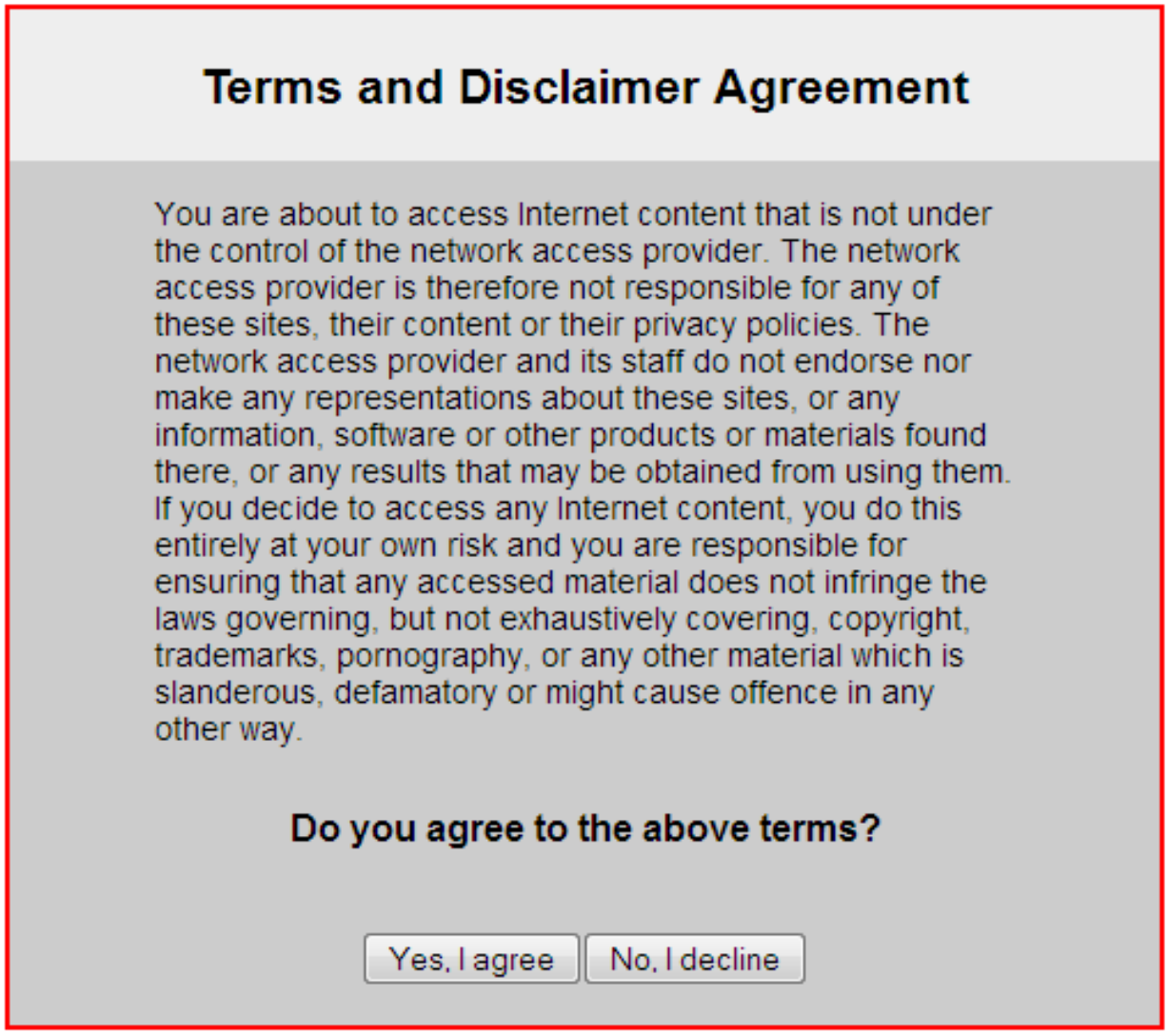
There is an exception to this rule. The line “Please enter your credentials to continue” is provided by the %%QUESTION%% tag. You can replace this tag with text of your choice. Except for this item, you should not remove any tags because they may carry information that the FortiGate unit needs.

- **Login failed page**—reports that the entered credentials were incorrect and enables the user to try again.

The Login failed page is similar to the Login page. It even contains the same login form. You can change any text that is not part of the HTML code nor a special tag enclosed in double percent (%) characters.

There is an exception to this rule. The line “Firewall authentication failed. Please try again.” is provided by the %%FAILED_MESSAGE%% tag. You can replace this tag with text of your choice. Except for this item, you should not remove any tags because they may carry information that the FortiGate unit needs.

- **Disclaimer page**—is a statement of the legal responsibilities of the user and the host organization to which the user must agree before proceeding.(WiFi or SSL VPN only)



- **Declined disclaimer page**—is displayed if the user does not agree to the statement on the Disclaimer page. Access is denied until the user agrees to the disclaimer.

Changing images in portal messages

You can replace the default Fortinet logo with your organization's logo. First, import the logo file into the FortiGate unit and then modify the Login page code to reference your file.

To import a logo file:

1. Go to **System > Config > Replacement Messages** and select **Manage Images**.
2. Select **Create New**.
3. Enter a **Name** for the logo and select the appropriate **Content Type**.
   The file must not exceed 24 Kilo bytes.
4. Select **Browse**, find your logo file and then select **Open**.
5. Select **OK**.

To specify the new logo in the replacement message:

1. Go to **System > Network > Interfaces** and edit the interface.
   The **Security Mode** must be **Captive Portal**.
2. Select the portal message to edit.
   - In SSL VPN or WiFi interfaces, in **Customize Portal Messages** click the link to the portal messages that you want to edit.
   - In other interfaces, make sure that **Customize Portal Messages** is selected, select the adjacent **Edit** icon, then select the message that you want to edit.
3. In the HTML message text, find the %%IMAGE tag.
   By default it specifies the Fortinet logo: `%%IMAGE:logo_fw_auth%%`
4. Change the image name to the one you provided for your logo.
   The tag should now read, for example, `%%IMAGE:mylogo%%`
5. Select **Save**.
6. Select **OK**.

Modifying text in portal messages

Generally, you can change any text that is not part of the HTML code nor a special tag enclosed in double percent (%) characters. You should not remove any tags because they may carry information that the FortiGate unit needs. See the preceding section for any exceptions to this rule for particular pages.

To modify portal page text

1. Go to **System > Network > Interfaces** and edit the interface.
   The SSID **Security Mode** must be **Captive Portal**.
2. Select the portal message to edit.
   - In SSL VPN or WiFi interfaces, in **Customize Portal Messages** click the link to the portal messages that you want to edit.
   - In other interfaces, make sure that **Customize Portal Messages** is selected, select the adjacent **Edit** icon, then select the message that you want to edit.
3. Edit the HTML message text, then select **Save**.
4. Select **OK**.

Certificate-based authentication

This section provides an overview of how the FortiGate unit verifies the identities of administrators, SSL VPN users, or IPsec VPN peers using X.509 security certificates.

The following topics are included in this section:

What is a security certificate?

A security certificate is a small text file that is part of a third-party generated public key infrastructure (PKI) to help guarantee the identity of both the user logging on and the web site they where they are logging in.

A certificate includes identifying information such as the company and location information for the web site, as well as the third-party company name, the expiry date of the certificate, and the public key.

FortiGate units use X.509 certificates to authenticate single sign-on (SSO) for users. The X.509 standard has been in use since before 2000, but has gained popularity with the Internet's increased popularity. X.509 v3 is defined in RFC 5280 and specifies standard formats for public key certificates, certificate revocation lists, and a certification path validation algorithm. The unused earlier X.509 version 1 was defined in RFC 1422.

The main difference between X.509 and PGP certificates is that where in PGP anyone can sign a certificate, for X.509 only a trusted authority can sign certificates. This limits the source of certificates to well known and trustworthy sources. Where PGP is well suited for one-to-one communications, the X.509 infrastructure is intended to be used in many different situations including one-to-many communications. Some common filename extensions for X.509 certificates are listed below.

Common certificate filename extensions

Filetype	Format name	Description
.pem	Privacy Enhanced Mail (PEM)	Base64 encoded DER certificate, that uses: "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----"
.cer **.crt** **.der**	Security CERtificate	Usually binary DER form, but Base64-encoded certificates are common too.
.p7b **.p7c**		Structure without data, just certificates or CRLs. PKCS#7 is a standard for signing or encrypting (officially called "enveloping") data.
.p12	PKCS#12	May contain certificate(s) (public) and private keys (password protected).
.pfx	personal information exchange (PFX)	Older format. Came before PKCS#12. Usually today data is in PKCS#12 format.

Certificates overview

Certificates play a major role in authentication of clients connecting to network services via HTTPS, both for administrators and SSL VPN users. Certificate authentication is optional for IPsec VPN peers.

- Certificates and protocols
- IPsec VPNs and certificates
- Certificate types on the FortiGate unit

Certificates and protocols

There are a number of protocols that are commonly used with certificates including SSL and HTTPS, and other certificate-related protocols.

SSL and HTTPS

The secure HTTP (HTTPS) protocol uses SSL. Certificates are an integral part of SSL. When a web browser connects to the FortiGate unit via HTTPS, a certificate is used to verify the FortiGate unit's identity to the client. Optionally, the FortiGate unit can require the client to authenticate itself in return.

By default, the FortiGate unit uses a self-signed security certificate to authenticate itself to HTTPS clients. When the certificate is offered, the client browser displays two security messages.

- The first message prompts users to accept and optionally install the FortiGate unit's self-signed security certificate. If the user does not accept the certificate, the FortiGate unit refuses the connection. When the user accepts the certificate, the FortiGate login page is displayed, and the credentials entered by the user are encrypted before they

are sent to the FortiGate unit. If the user chooses to install the certificate, the prompt is not displayed again.

- Just before the FortiGate login page is displayed, a second message informs users that the FortiGate certificate distinguished name differs from the original request. This message is displayed because the FortiGate unit redirects the connection (away from the distinguished name recorded in the self-signed certificate) and can be ignored.

Optionally, you can install an X.509 server certificate issued by a certificate authority (CA) on the FortiGate unit. You can then configure the FortiGate unit to identify itself using the server certificate instead of the self-signed certificate.

For more information, see the FortiOS Handbook SSL VPN guide.

After successful certificate authentication, communication between the client browser and the FortiGate unit is encrypted using SSL over the HTTPS link.

Certificate-related protocols

There are multiple protocols that are required for handling certificates. These include the Online Certificate Status Protocol (OCSP), Secure Certificate Enrollment Protocol (SCEP), and Server-based Certificate Validation Protocol (SCVP).

Online Certificate Status Protocol

Online Certificate Status Protocol (OCSP) allows the verification of X.509 certificate expiration dates. This is important to prevent hackers from changing the expiry date on an old certificate to a future date.

Normally certificate revocation lists (CRLs) are used, but OCSP is an alternate method available. However a CRL is a public list, and some companies may want to avoid the public exposure of their certificate structure even if it is only invalid certificates.

The OSCP check on the certificate's revocation status is typically carried out over HTTP with a request-response format. The authority responding can reply with a status of good, revoked, or unknown for the certificate in question.

Secure Certificate Enrollment Protocol

Secure Certificate Enrollment Protocol (SCEP) is an automated method of signing up for certificates. Typically this involves generating a request you send directly to the SCEP service, instead of generating a file request that may or may not be signed locally.

Server-based Certificate Validation Protocol

Server-based Certificate Validation Protocol (SCVP) is used to trace a certificate back to a valid root level certificate. This ensures that each step along the path is valid and trustworthy.

IPsec VPNs and certificates

Certificate authentication is a more secure alternative to preshared key (shared secret) authentication for IPsec VPN peers. Unlike administrators or SSL VPN users, IPsec peers use HTTP to connect to the VPN gateway configured on the FortiGate unit. The VPN gateway configuration can require certificate authentication before it permits an IPsec tunnel to be established. See Authenticating IPsec VPN users with security certificates on page 108 .

Certificate types on the FortiGate unit

There are different types of certificates available that vary depending on their intended use. FortiOS supports local, remote, CA, and CRL certificates.

Local certificates

Local certificates are issued for a specific server, or web site. Generally they are very specific, and often for an internal enterprise network. For example a personal web site for John Smith at www.example.com (such as http://www.example.com/home/jsmith) would have its own local certificate.

These can optionally be just the certificate file, or also include a private key file and PEM passphrase for added security.

For information about generating a certificate request, see Generating a certificate signing request on page 99. For information about installing a local certificate, see Obtaining and installing a signed server certificate from an external CA on page 102

Remote certificates

Remote certificates are public certificates without a private key. For dynamic certificate revocation, you need to use an Online Certificate Status Protocol (OCSP) server. The OCSP is configured in the CLI only. Installed Remote (OCSP) certificates are displayed in the Remote Certificates list. You can select **Import** to install a certificate from the management PC.

CA root certificates

CA root certificates are similar to local certificates, however they apply to a broader range of addresses or to whole company; they are one step higher up in the organizational chain. Using the local certificate example, a CA root certificate would be issued for all of www.example.com instead of just the smaller single web page.

Certificate revocation list

Certificate revocation list (CRL) is a list of certificates that have been revoked and are no longer usable. This list includes certificates that have expired, been stolen, or otherwise compromised. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and includes the date and time when the next CRL will be issued as well as a sequence number to help ensure you have the most current version of the CRL.

Certificate signing

The trust in a certificate comes from the authority that signs it. For example if VeriSign signs your CA root certificate, it is trusted by everyone. While these certificates are universally accepted, it is cumbersome and expensive to have all certificates on a corporate network signed with this level of trust.

With self-signed certificates nobody, except the other end of your communication, knows who you are and therefore they do not trust you as an authority. However this level is useful for encryption between two points — neither point may care about who signed the certificate, just that it allows both points to communicate. This is very useful for internal networks and communications.

A general rule is that CA signed certificates are accepted and sometimes required, but it is easier to self-sign certificates when you are able.

For more on the methods of certificate signing see Generating a certificate signing request on page 99.

Managing X.509 certificates

Managing security certificates is required due to the number of steps involved in both having a certificate request signed, and then distributing the correct files for use.

You use the FortiGate unit or CA software such as OpenSSL to generate a certificate request. That request is a text file that you send to the CA for verification, or alternately you use CA software to self-validate. Once validated, the certificate file is generated and must be imported to the FortiGate unit before it can be used. These steps are explained in more detail later in this section.

This section provides procedures for generating certificate requests, installing signed server certificates, and importing CA root certificates and CRLs to the FortiGate unit.

For information about how to install root certificates, CRLs, and personal or group certificates on a remote client browser, refer to your browser's documentation.

This section includes:

Generating a certificate signing request

Whether you create certificates locally with a software application or obtain them from an external certificate service, you will need to generate a certificate signing request (CSR).

When you generate a CSR, a private and public key pair is created for the FortiGate unit. The generated request includes the public key of the FortiGate unit and information such as the FortiGate unit's public static IP address, domain name, or email address. The FortiGate unit's private key remains confidential on the FortiGate unit.

After you submit the request to a CA, the CA will verify the information and register the contact information on a digital certificate that contains a serial number, an expiration date, and the public key of the CA. The CA will then sign the certificate, and you install the certificate on the FortiGate unit.

The Certificate Request Standard is a public key cryptography standard (PKCS) published by RSA, specifically PKCS10 which defines the format for CSRs. This is defined in RFC 2986.

To generate a certificate request in FortiOS - web-based manager:

1. Go to **System > Certificates > Local Certificates**.
2. Select **Generate**.
3. In the **Certificate Name** field, enter a unique meaningful name for the certificate request. Typically, this would be the hostname or serial number of the FortiGate unit or the domain of the FortiGate unit such as example.com.

Do not include spaces in the certificate name. This will ensure compatibility of a signed certificate as a PKCS12 file to be exported later on if required.

4. Enter values in the **Subject Information** area to identify the FortiGate unit:
   - If the FortiGate unit has a static IP address, select **Host IP**and enter the public IP address of the FortiGate unit. If the FortiGate unit does not have a public IP address, use an email address (or fully qualified domain name (FQDN) if available) instead.
   - If the FortiGate unit has a dynamic IP address and subscribes to a dynamic DNS service, use a FQDN if available to identify the FortiGate unit. If you select **Domain Name**, enter the FQDN of the FortiGate unit. Do not include the protocol specification (http://) or any port number or path names.

If a domain name is not available and the FortiGate unit subscribes to a dynamic DNS service, an “unable to verify certificate” type message may be displayed in the user’s browser whenever the public IP address of the FortiGate unit changes.

   - If you select **E-Mail**, enter the email address of the owner of the FortiGate unit.
5. Enter values in the **Optional Information** area to further identify the FortiGate unit.

Organization Unit	Name of your department. You can enter a series of OUs up to a maximum of 5. To add or remove an OU, use the plus (+) or minus (-) icon.
Organization	Legal name of your company or organization.
Locality (City)	Name of the city or town where the FortiGate unit is installed.
State/Province	Name of the state or province where the FortiGate unit is installed.
Country	Select the country where the FortiGate unit is installed.
e-mail	Contact email address.
Subject Alternative Name	Optionally, enter one or more alternative names for which the certificate is also valid. Separate names with a comma. A name can be: • e-mail address • IP address • URI • DNS name (alternatives to the Common Name) • directory name (alternatives to the Distinguished Name) You must precede the name with the name type. Examples: IP:1.1.1.1 email:test@fortinet.com email:my@other.address URI:http://my.url.here/

6. From the **Key Type** list, select **RSA** or **Elliptic Curve**.
7. From the **Key Size** list, select **1024 Bit**, **1536 Bit**, **2048 Bit** or **secp256r1**, **secp384r1**, **secp521r1** respectively. Larger keys are slower to generate but more secure.
8. In **Enrollment Method**, you have two methods to choose from. Select **File Based** to generate the certificate request, or **Online SCEP** to obtain a signed SCEP-based certificate automatically over the network. For the SCEP method, enter the URL of the SCEP server from which to retrieve the CA certificate, and the CA server challenge password.
9. Select **OK**.
10. The request is generated and displayed in the **Local Certificates** list with a status of `PENDING`.
11. Select the **Download** button to download the request to the management computer.
12. In the **File Download** dialog box, select **Save** and save the Certificate Signing Request on the local file system of the management computer.
13. Name the file and save it on the local file system of the management computer.

The certificate request is ready for the certificate authority to be signed.

Generating certificates with CA software

CA software allows you to generate unmanaged certificates and CA certificates for managing other certificates locally without using an external CA service. Examples of CA software include ssl-ca from OpenSSL (available for Linux, Windows, and Mac) or gensslcert from SuSE, MS Windows Server 2000 and 2003 come with a CA as part of their certificate services, and in MS Windows 2008 CA software can be installed as part of the Active Directory installation. See Example — Generate and Import CA certificate with private key pair on OpenSSL on page 110.

The general steps for generating certificates with CA software are

1. Install the CA software as a stand-alone root CA.
2. Provide identifying information for your self-administered CA.

While following these steps, the methods vary slightly when generating server certificates, CA certificates, and PKI certificates.

Server certificate

1. Generate a Certificate Signing Request (CSR) on the FortiGate unit.
2. Copy the CSR base-64 encoded text (PKCS10 or PKCS7) into the CA software and generate the certificate. PKCS10 is the format used to send the certificate request to the signing authority. PKCS7 is the format the signing authority can use for the newly signed certificate.
3. Export the certificate as a X.509 DER encoded binary file with .CER extension
4. Upload the certificate file to the FortiGate unit Local Certificates page (type is Certificate).

CA certificate

1. Retrieve the CA Certificate from the CA software as a DER encoded file.
2. Import the CA certificate file to the FortiGate unit at **System > Certificates > Import > CA Certificates**.

PKI certificate

1. Generate a Certificate Signing Request (CSR) on the FortiGate unit.
2. Copy the CSR base-64 encoded text (PKCS#10 or PKCS#7) into the CA software and generate the certificate. PKCS10 is the format used to send the certificate request to the signing authority. PKCS7 is the format the signing authority can use for the newly signed certificate.

3. Export the certificate as a X.509 DER encoded binary file with .CER extension.
4. Install the certificate in the user's web browser or IPsec VPN client as needed.

Obtaining and installing a signed server certificate from an external CA

To obtain a signed server certificate for a FortiGate unit, you must send a request to a CA that provides digital certificates that adhere to the X.509 standard. The FortiGate unit provides a way for you to generate the request.

To submit the certificate signing request (file-based enrollment):

1. Using the web browser on the management computer, browse to the CA web site.
2. Follow the CA instructions for a base-64 encoded PKCS#10 certificate request and upload your certificate request.
3. Follow the CA instructions to download their root certificate and CRL.
   When you receive the signed server certificate from the CA, install the certificate on the FortiGate unit.

To install or import the signed server certificate - web-based manager

1. On the FortiGate unit, go to **System > Certificates > Import > Local Certificates**.
2. From **Type**, select **Local Certificate**.
3. Select **Browse**, browse to the location on the management computer where the certificate was saved, select the certificate, and then select **Open**.
4. Select **OK**, and then select **Return**.

Installing a CA root certificate and CRL to authenticate remote clients

When you apply for a signed personal or group certificate to install on remote clients, you can obtain the corresponding root certificate and CRL from the issuing CA. When you receive the signed personal or group certificate, install the signed certificate on the remote client(s) according to the browser documentation. Install the corresponding root certificate (and CRL) from the issuing CA on the FortiGate unit according to the procedures given below.

To install a CA root certificate

1. After you download the root certificate of the CA, save the certificate on the management computer. Or, you can use online SCEP to retrieve the certificate.
2. On the FortiGate unit, go to **System > Certificates > Import > CA Certificates**.
3. Do one of the following:
   - To import using SCEP, select **SCEP**. Enter the URL of the SCEP server from which to retrieve the CA certificate. Optionally, enter identifying information of the CA, such as the filename.
   - To import from a file, select **Local PC**, then select **Browse** and find the location on the management computer where the certificate has been saved. Select the certificate, and then select **Open**.
5. Select **OK**, and then select **Return**.

The system assigns a unique name to each CA certificate. The names are numbered consecutively (CA_Cert_1, CA_Cert_2, CA_Cert_3, and so on).

To import a certificate revocation list

A Certificate Revocation List (CRL) is a list of the CA certificate subscribers paired with certificate status information. The list contains the revoked certificates and the reason(s) for revocation. It also records the certificate issue dates and the CAs that issued them.

When configured to support SSL VPNs, the FortiGate unit uses the CRL to ensure that the certificates belonging to the CA and remote peers or clients are valid. The CRL has an “effective date” and a “next update” date. The interval is typically 7 days (for Microsoft CA). FortiOS will update the CRL automatically. Also, there is a CLI command to specify an “update-interval” in seconds. Recommendation should be 24 hours (86400 seconds) but depends on company security policy.

1. After you download the CRL from the CA web site, save the CRL on the management computer.
2. Go to **System > Certificates > Import > CRL**.
3. Do one of the following:
   - To import using an HTTP server, select **HTTP** and enter the URL of the HTTP server.
   - To import using an LDAP server see this KB article.
   - To import using an SCEP server, select **SCEP** and select the Local Certificate from the list. Enter the URL of the SCEP server from which the CRL can be retrieved.
   - To import from a file, select **Local PC**, then select **Browse** and find the location on the management computer where the CRL has been saved. Select the CRL and then select **Open**.
5. Select **OK**, and then select **Return**.

Troubleshooting certificates

There are times when there are problems with certificates — a certificate is seen as expired when its not, or it can’t be found. Often the problem is with a third party web site, and not FortiOS. However, some problems can be traced back to FortiOS such as DNS or routing issues.

Certificate is reported as expired when it is not

Certificates often are issued for a set period of time such as a day or a month, depending on their intended use. This ensures everyone is using up-to-date certificates. It is also more difficult for hackers to steal and use old certificates.

Reasons a certificate may be reported as expired include:

- It really has expired based on the “best before” date in the certificate
- The FortiGate unit clock is not properly set. If the FortiGate clock is fast, it will see a certificate as expired before the expiry date is really here.
- The requesting server clock is not properly set. A valid example is if your certificate is 2 hours from expiring, a server more than two time zones away would see the certificate as expired. Otherwise, if the server’s clock is set wrongly it will also have the same effect.
- The certificate was revoked by the issuer before the expiry date. This may happen if the issuer believes a certificate was either stolen or misused. Its possible it is due to reasons on the issuer’s side, such as a system change or such. In either case it is best to contact the certificate issuer to determine what is happening and why.

A secure connection cannot be completed (Certificate cannot be found)

Everyone who uses a browser has encountered a message such as *This connection is untrusted*. Normally when you try to connect securely to a web site, that web site will present its valid certificate to prove their identity is valid. When the web site's certificate cannot be verified as valid, the message appears stating *This connection is untrusted* or something similar. If you usually connect to this web site without problems, this error could mean that someone is trying to impersonate or hijack the web site, and best practices dictates you not continue.

Reasons a web site's certificate cannot be validated include:

- The web site uses an unrecognized self-signed certificate. These are not secure because anyone can sign them. If you accept self-signed certificates you do so at your own risk. Best practices dictate that you must confirm the ID of the web site using some other method before you accept the certificate.
- The certificate is valid for a different domain. A certificate is valid for a specific location, domain, or sub-section of a domain such as one certificate for `support.example.com` that is not valid for `marketing.example.com`. If you encounter this problem, contact the webmaster for the web site to inform them of the problem.
- There is a DNS or routing problem. If the web site's certificate cannot be verified, it will not be accepted. Generally to be verified, your system checks with the third party certificate signing authority to verify the certificate is valid. If you cannot reach that third party due to some DNS or routing error, the certificate will not be verified.
- Firewall is blocking required ports. Ensure that any firewalls between the requesting computer and the web site allow the secure traffic through the firewall. Otherwise a hole must be opened to allow it through. This includes ports such as 443 (HTTPS) and 22 (SSH).

Online updates to certificates and CRLs

If you obtained your local or CA certificate using SCEP, you can configure online renewal of the certificate before it expires. Similarly, you can receive online updates to CRLs.

Local certificates

In the `config vpn certificate local` command, you can specify automatic certificate renewal. The relevant fields are:

`scep-url <URL_str>`	The URL of the SCEP server. This can be HTTP or HTTPS. The following options appear after you add the `<URL_str>`.
`scep-password <password_str>`	The password for the SCEP server.
`auto-regenerate-days <days_int>`	How many days before expiry the FortiGate unit requests an updated local certificate. The default is `0`, no auto-update.
`auto-regenerate-days-warning <days_int>`	How many days before local certificate expiry the FortiGate generates a warning message. The default is `0`, no warning.

In this example, an updated certificate is requested three days before it expires.

```
config vpn certificate local
   edit mycert
      set scep-url http://scep.example.com/scep
      set scep-server-password my_pass_123
      set auto-regenerate-days 3
      set auto-regenerate-days-warning 2
```

```
end
```

CA certificates

In the `config vpn certificate ca` command, you can specify automatic certificate renewal. The relevant fields are:

Variable	Description
`scep-url <URL_str>`	The URL of the SCEP server. This can be HTTP or HTTPS.
`auto-update-days <days_int>`	How many days before expiry the FortiGate unit requests an updated CA certificate. The default is `0`, no auto-update.
`auto-update-days-warning <days_int>`	How many days before CA certificate expiry the FortiGate generates a warning message. The default is `0`, no warning.

In this example, an updated certificate is requested three days before it expires.

```
config vpn certificate ca
   edit mycert
      set scep-url http://scep.example.com/scep
      set auto-update-days 3
      set auto-update-days-warning 2
   end
```

Certificate Revocation Lists

If you obtained your CRL using SCEP, you can configure online updates to the CRL using the `config vpn certificate crl` command. The relevant fields are:

Variable	Description
`http-url <http_url>`	URL of the server used for automatic CRL certificate updates. This can be HTTP or HTTPS.
`scep-cert <scep_certificate>`	Local certificate used for SCEP communication for CRL auto-update.
`scep-url <scep_url>`	URL of the SCEP CA server used for automatic CRL certificate updates. This can be HTTP or HTTPS.
`update-interval <seconds>`	How frequently, in seconds, the FortiGate unit checks for an updated CRL. Enter `0` to update the CRL only when it expires. Not available for http URLs.
`update-vdom <update_vdom>`	VDOM used to communicate with remote SCEP server for CRL auto-update.

In this example, an updated CRL is requested only when it expires.

```
config vpn certificate crl
   edit cert_crl
      set http-url http://scep.example.com/scep
```

```
    set scep-cert my-scep-cert
    set scep-url http://scep.ca.example.com/scep
    set update-interval 0
    set update-vdom root
end
```

Backing up and restoring local certificates

The FortiGate unit provides a way to export and import a server certificate and the FortiGate unit's personal key through the CLI. If required (to restore the FortiGate unit configuration), you can import the exported file through the **System > Certificates** page of the web-based manager.

As an alternative, you can back up and restore the entire FortiGate configuration through the **System Information** widget on the Dashboard of the web-based manager. Look for **[Backup]** and **[Restore]** in the **System Configuration** row. The backup file is created in a FortiGate-proprietary format.

To export a server certificate and private key - CLI:

This procedure exports a server (local) certificate and private key together as a password protected PKCS12 file. The export file is created through a customer-supplied TFTP server. Ensure that your TFTP server is running and accessible to the FortiGate unit before you enter the command.

1. Connect to the FortiGate unit through the CLI.
2. Type the following command:

```
execute vpn certificate local export tftp <cert_name> <exp_filename> <tftp_ip>
    <password>
```

   where:

   - `<cert_name>` is the name of the server certificate; typing `?` displays a list of installed server certificates.
   - `<exp_filename>` is a name for the output file.
   - `<tftp_ip>` is the IP address assigned to the TFTP server host interface.
3. Move the output file from the TFTP server location to the management computer for future reference.

To import a server certificate and private key - web-based manager:

1. Go to **System > Certificates** and select **Import**.
2. In **Type**, select **PKCS12 Certificate**.
3. Select **Browse**. Browse to the location on the management computer where the exported file has been saved, select the file, and then select **Open**.
4. In the **Password** field, type the password needed to upload the exported file.
5. Select **OK**, and then select **Return**.

To import separate server certificate and private key files - web-based manager

Use the following procedure to import a server certificate and the associated private key file when the server certificate request and private key were not generated by the FortiGate unit. The two files to import must be available on the management computer.

1. Go to **System > Certificates** and select **Import**.
2. In **Type**, select **Certificate**.

3. Select the **Browse** button beside the **Certificate file** field. Browse to the location on the management computer where the certificate file has been saved, select the file, and then select **Open**.
4. Select the **Browse** button beside the **Key file** field. Browse to the location on the management computer where the key file has been saved, select the file, and then select **Open**.
5. If required, in the **Password** field, type the associated password, and then select **OK**.
6. Select **Return**.

Configuring certificate-based authentication

You can configure certificate-based authentication for FortiGate administrators, SSL VPN users, and IPsec VPN users.

In Microsoft Windows 7, you can use the certificate manager to keep track of all the different certificates on your local computer. To access certificate manager, in Windows 7 press the Windows key, enter “certmgr.msc” at the search prompt, and select the displayed match. Remember that in addition to these system certificates, many applications require you to register certificates with them directly.

To see FortiClient certificates, open the FortiClient Console, and select VPN. The VPN menu has options for My Certificates (local or client) and CA Certificates (root or intermediary certificate authorities). Use Import on those screens to import certificate files from other sources.

Authenticating administrators with security certificates

You can install a certificate on the management computer to support strong authentication for administrators. When a personal certificate is installed on the management computer, the FortiGate unit processes the certificate after the administrator supplies a username and password.

To enable strong administrative authentication:

- Obtain a signed personal certificate for the administrator from a CA and load the signed personal certificate into the web browser on the management computer according to the browser documentation.
- Install the root certificate and the CRL from the issuing CA on the FortiGate unit (see Installing a CA root certificate and CRL to authenticate remote clients on page 102).
- Create a PKI user account for the administrator.
- Add the PKI user account to a firewall user group dedicated to PKI-authenticated administrators.
- In the administrator account configuration, select **PKI** as the account **Type** and select the **User Group** to which the administrator belongs.

Authenticating SSL VPN users with security certificates

While the default self-signed certificates can be used for HTTPS connections, it is preferable to use the X.509 server certificate to avoid the redirection as it can be misinterpreted as possible session hijacking. However, the server certificate method is more complex than self-signed security certificates. Also the warning message is typically displayed for the initial connection, and future connections will not generate these messages.

X.509 certificates can be used to authenticate IPsec VPN peers or clients, or SSL VPN clients. When configured to authenticate a VPN peer or client, the FortiGate unit prompts the VPN peer or client to authenticate itself using the X.509 certificate. The certificate supplied by the VPN peer or client must be verifiable using the root CA certificate installed on the FortiGate unit in order for a VPN tunnel to be established.

To enable certificate authentication for an SSL VPN user group:

1. Install a signed server certificate on the FortiGate unit and install the corresponding root certificate (and CRL) from the issuing CA on the remote peer or client.
2. Obtain a signed group certificate from a CA and load the signed group certificate into the web browser used by each user. Follow the browser documentation to load the certificates.
3. Install the root certificate and the CRL from the issuing CA on the FortiGate unit (see Installing a CA root certificate and CRL to authenticate remote clients on page 102).
4. Create a PKI user for each SSL VPN user. For each user, specify the text string that appears in the Subject field of the user's certificate and then select the corresponding CA certificate.
5. Use the `config user peergrp` CLI command to create a peer user group. Add to this group all of the SSL VPN users who are authenticated by certificate.
6. Go to **Policy & Objects > Policy > IPv4**.
7. Edit the SSL-VPN security policy.
8. Select the user group created earlier in the **Source User(s)** field.
9. Select **OK**.

Authenticating IPsec VPN users with security certificates

To require VPN peers to authenticate by means of a certificate, the FortiGate unit must offer a certificate to authenticate itself to the peer.

To enable the FortiGate unit to authenticate itself with a certificate:

1. Install a signed server certificate on the FortiGate unit.
   See To install or import the signed server certificate - web-based manager on page 102.
2. Install the corresponding CA root certificate on the remote peer or client. If the remote peer is a FortiGate unit, see To install a CA root certificate on page 102.
3. Install the certificate revocation list (CRL) from the issuing CA on the remote peer or client. If the remote peer is a FortiGate unit, see To import a certificate revocation list on page 103.
4. In the VPN phase 1 configuration, set **Authentication Method** to **Signature** and from the **Certificate Name** list select the certificate that you installed in Step 1.

To authenticate a VPN peer using a certificate, you must install a signed server certificate on the peer. Then, on the FortiGate unit, the configuration depends on whether there is only one VPN peer or if this is a dialup VPN that can be multiple peers.

To configure certificate authentication of a single peer

1. Install the CA root certificate and CRL.
2. Create a PKI user to represent the peer. Specify the text string that appears in the Subject field of the user's certificate and then select the corresponding CA certificate.
3. In the VPN phase 1 **Peer Options**, select **peer certificate** for **Accept Types** field and select the PKI user that you created in the **Peer certificate** field.

To configure certificate authentication of multiple peers (dialup VPN)

1. Install the corresponding CA root certificate and CRL.
2. Create a PKI user for each remote VPN peer. For each user, specify the text string that appears in the Subject field of the user's certificate and then select the corresponding CA certificate.
3. Use the `config user peergrp` CLI command to create a peer user group. Add to this group all of the PKI users who will use the IPsec VPN.

In the VPN phase 1 **Peer Options**, select **peer certificate group** for **Accept Types** field and select the PKI user group that you created in the **Peer certificate group** field.

Example — Generate a CSR on the FortiGate unit

This example follows all the steps required to create and install a local certificate on the FortiGate unit, without using CA software.

The FortiGate unit is called myFortiGate60, and is located at 10.11.101.101 (a private IP address) and http://myfortigate.example.com. Mr. John Smith (john.smith@myfortigate.example.com) is the IT administrator for this FortiGate unit, and the unit belongs to the Sales department located in Greenwich, London, England.

To generate a certificate request on the FortiGate unit - web-based manager:

1. Go to **System > Certificates**.
2. Select **Generate**.
3. In the **Certificate Name** field, enter `myFortiGate60`.

Do not include spaces in the certificate name. This will ensure compatibility of a signed certificate as a PKCS12 file to be exported later on if required.

Since the IP address is private, we will use the FQDN instead.

4. Select **Domain Name**, and enter `http://myfortigate.example.com`.
5. Enter values in the **Optional Information** area to further identify the FortiGate unit.

Organization Unit	Sales
Organization	Example.com
Locality (City)	Greenwich
State/Province	London
Country	England
e-mail	john.smith@myfortigate.example.com

6. From the **Key Type** list, select **RSA** or **Elliptic Curve**.
7. If RSA is selected, from the **Key Size** list, select **2048 Bit**. If Elliptic Curve is selected,from the **Curve Name** list, select **secp256r1**.
8. In **Enrollment Method**, select **File Based** to generate the certificate request
9. Select **OK**.
   The request is generated and displayed in the **Local Certificates** list with a status of PENDING.
10. Select the **Download** button to download the request to the management computer.
11. In the **File Download** dialog box, select ***Save*** and save the Certificate Signing Request on the local file system of the management computer.
12. Name the file and save it on the local file system of the management computer.

Example — Generate and Import CA certificate with private key pair on OpenSSL

This example explains how to generate a certificate using OpenSSL on MS Windows. OpenSSL is available for Linux and Mac OS as well, however their terminology will vary slightly from what is presented here.

Assumptions

Before starting this procedure, ensure that you have downloaded and installed OpenSSL on Windows. One source is: http://www.slproweb.com/products/Win32OpenSSL.html.

Generating and importing the CA certificate and private key

The two following procedures will generate a CA certificate file and private key file, and then import it to the FortiGate unit as a local certificate.

To generate the private key and certificate

1. At the Windows command prompt, go to the OpenSSL bin directory. If you installed to the default location this will be the command:
   ```
   cd c:\OpenSSL-Win32\bin
   ```
2. Enter the following command to generate the private key. You will be prompted to enter your PEM pass phrase. Choose something easy to remember such as fortinet123.
   ```
   openssl genrsa -des3 -out fgtcapriv.key 2048
   ```
   This command generates an RSA DES3 2048-bit encryption key.
3. The following command will generate the certificate using the key from the previous step.
   ```
   openssl req -new -x509 -days 3650 -extensions v3_ca -key fgtcapriv.key -out
       fgtca.crt
   ```
   This step generates an X509 CA certificate good for 10 years that uses the key generated in the previous step. The certificate filename is `fgtca.crt`.

   You will be prompted to enter information such as PEM Pass Phrase from the previous step, Country Name, State, Organization Name, Organizational Unit (such as department name), Common Name (the FQDN), and Email Address.

To import the certificate to the FortiGate unit - web-based manager:

1. Go to **System > Certificates**.
2. Select **Import > Local Certificate**.
3. Select **Certificate** for **Type**.
   Fields for Certificate file, Key file, and Password are displayed.
4. For **Certificate file**, enter `c:\OpenSSL-Win32\bin\fgtca.crt`.
5. For **Key file**, enter `c:\OpenSSL-Win32\bin\fgtcapriv.key`.
6. For **Password**, enter the PEM Pass Phrase you entered earlier, such as fortinet123.
7. Select **OK**.

The Certificate will be added to the list of Local Certificates and be ready for use. It will appear in the list as the filename you uploaded — `fgtca`.You can add comments to this certificate to make it clear where its from and how it is intended to be used. If you download the certificate from FortiOS, it is a .CER file.

It can now be used in Authenticating IPsec VPN users with security certificates on page 108, and Authenticating SSL VPN users with security certificates on page 107.

Optionally, you can install the certificate as a CA Certificate. CA certificates are used in HTTPS proxy/inspection. To do this, under **System > Certificates** select **Import > CA Certificate**. Select **Local PC** and enter the certificate file `c:\OpenSSL-Win32\bin\fgtca.crt`. Then select **OK**. This certificate will be displayed in the CA Certificate list under the name `CA_Cert_1`.

Example — Generate an SSL certificate in OpenSSL

This example explains how to generate a CA signed SSL certificate using OpenSSL on MS Windows. OpenSSL is available for Linux and Mac OS as well, however their terminology will vary slightly from what is presented here.

In this example, you will:

- Generate a CA signed SSL certificate
- Generate a self-signed SSL certificate
- Import the SSL certificate into FortiOS

Assumptions

- Before starting this procedure, ensure that you have downloaded and installed OpenSSL on MS Windows. One download source is http://www.slproweb.com/products/Win32OpenSSL.html.

Generating a CA signed SSL certificate

This procedure assumes that you have already completed Example — Generate and Import CA certificate with private key pair on OpenSSL on page 110 successfully.

To generate the CA signed SSL certificate:

1. At the Windows command prompt, go to the OpenSSL bin directory. If you installed to the default location this will be the following command:

```
cd c:\OpenSSL-Win32\bin
```

2. Enter the following command to generate the private key. You will be prompted to enter your PEM pass phrase. Choose something easy to remember such as fortinet.

```
openssl genrsa -des3 -out fgtssl.key 2048
```

This command generates an RSA DES3 2048-bit encryption key.

3. Create a certificate signing request for the SSL certificate. This step requires you to enter the information listed in step 3 of the previous example — To generate the private key and certificate. You can leave the Challenge Password blank.

```
openssl req -new -key fgtssl.key -out fgtssl.csr
```

4. Using the CSR from the previous step, you can now create the SSL certificate using the CA certificate that was created in Example — Generate and Import CA certificate with private key pair on OpenSSL.

```
openssl x509 -req -days 365 -in fgtssl.csr -CA fgtca.crt -CAkey fgtcapriv.key -set_
    serial 01 -out fgtssl.crt
```

This will generate an X.509 certificate good for 365 days signed by the CA certificate fgtca.crt.

Generating a self-signed SSL certificate

This procedures does not require any existing certificates.

1. At the Windows command prompt, go to the OpenSSL bin directory. If you installed to the default location this will be the following command:

```
cd c:\OpenSSL-Win32\bin
```

2. Enter the following command to generate the private key. You will be prompted to enter your PEM pass phrase. Choose something easy to remember such as fortinet.

```
openssl genrsa -des3 -out fgtssl.key 2048
openssl req -new -key fgtssl.key -out fgtssl.csr
openssl x509 -req -days 365 -in fgtssl.csr -signkey fgtssl.key -out fgtssl.crt
```

These commands:

- generate an RSA 3DES 2048-bit private key,
- generate an SSL certificate signing request, and
- sign the CSR to generate an SSL .CRT certificate file.

Import the SSL certificate into FortiOS

To import the certificate to FortiOS- web-based manager

1. Go to **System > Certificates**.
2. Select **Import > Local Certificate**.
3. Select **Certificate** for **Type**.
   Fields for Certificate file, Key file, and Password are displayed.
4. For **Certificate file**, enter `c:\OpenSSL-Win32\bin\fgtssl.crt`.
5. For **Key file**, enter `c:\OpenSSL-Win32\bin\fgtssl.key`.
6. For **Password**, enter the PEM Pass Phrase you entered, such as fortinet.
7. Select **OK**.

The SSL certificate you just uploaded can be found under **System > Certificates** under the name of the file you uploaded — `fgtssl`.

To confirm the certificate is uploaded properly - CLI:

```
config vpn certificate local
   edit fgtssl
      get
   end
```

The get command will display all the certificate's information. If it is not there or the information is not correct, you will need to remove the corrupted certificate (if it is there) and upload it again from your PC.

To use the new SSL certificate - CLI

```
config vpn ssl settings
   set servercert fgtssl
end
```

This assigns the fgtssl certificate as the SSL server certificate. For more information see the FortiOS Handbook SSL VPN guide.

Single Sign-On using a FortiAuthenticator unit

If you use a FortiAuthenticator unit in your network as a single sign-on agent,

- Users can authenticate through a web portal on the FortiAuthenticator unit.
- Users with FortiClient Endpoint Security installed can be automatically authenticated by the FortiAuthenticator unit through the FortiClient SSO Mobility Agent.

The FortiAuthenticator unit can integrate with external network authentication systems such as RADIUS and LDAP to gather user logon information and send it to the FortiGate unit.

User's view of FortiAuthenticator SSO authentication

There are two different ways users can authenticate through a FortiAuthenticator unit.

Users without FortiClient Endpoint Security - SSO widget

To log onto the network, the user accesses the organization's web page with a web browser. Embedded on that page is a simple logon widget, like this:

	User not logged in. Click **Login** to go to the FortiAuthenticator login page.
	User logged in. Name displayed. **Logout** button available.

The SSO widget sets a cookie on the user's browser. When the user browses to a page containing the login widget, the FortiAuthenticator unit recognizes the user and updates its database if the user's IP address has changed. The user will not need to re-authenticate until the login timeout expires, which can be up to 30 days.

Users with FortiClient Endpoint Security - FortiClient SSO Mobility Agent

The user simply accesses resources and all authentication is performed transparently with no request for credentials. IP address changes, such as those due to WiFi roaming, are automatically sent to the FortiAuthenticator unit. When the user logs off or otherwise disconnects from the network, the FortiAuthenticator unit is aware of this and deauthenticates the user.

The FortiClient SSO Mobility Agent, a feature of FortiClient Endpoint Security v5.0, must be configured to communicate with the appropriate FortiAuthenticator unit. After that, the agent automatically provides user name and IP address information to the FortiAuthenticator unit for transparent authentication.

Administrator's view of FortiAuthenticator SSO authentication

You can configure either or both of these authentication types on your network.

SSO widget

You need to configure the Single Sign-On portal on the FortiAuthenticator unit. Go to **Fortinet SSO Methods > SSO > Portal Services** to do this. Copy the **Embeddable login widget** code for use on your organization's home page. Identity-based security policies on the FortiGate unit determine which users or groups of users can access which network resources.

FortiClient SSO Mobility Agent

Your users must be running at least FortiClient Endpoint Security v5.0 to make use of this type of authentication.

On the FortiAuthenticator unit, you need to select **Enable FortiClient SSO Mobility Agent Service**, optionally select **Enable Authentication** and choose a **Secret key**. Go to **Fortinet SSO Methods > SSO > General**. You need to provide your users the FortiAuthenticator IP address and secret key so that they can configure the FortiClient SSO Mobility Agent on their computers. See Configuring the FortiGate unit on page 116.

Configuring the FortiAuthenticator unit

The FortiAuthenticator unit can poll FortiGate units, Windows Active Directory, RADIUS servers, LDAP servers, and FortiClients for information about user logon activity.

To configure FortiAuthenticator polling:

1. Go to **Fortinet SSO Methods > SSO > General**.
2. In the **FortiGate** section, leave the Listening port at 8000, unless your network requires you to change this. The FortiGate unit must allow traffic on this port to pass through the firewall.
   Optionally, you can set the Login Expiry time. This is the length of time users can remain logged in before the system logs them off automatically. The default is 480 minutes (8 hours).
3. Select **Enable Authentication** and enter the **Secret key**. Be sure to use the same secret key when configuring the FSSO Agent on FortiGate units.
4. In the **Fortinet Single Sign-On (FSSO)** section, enter

Enable Windows Active Directory domain controllers	Select for integration with Windows Active Directory.
Enable Radius accounting SSO clients	Select if you want to use a Remote Radius server.
Enable Syslog SSO	Select for integration with Syslog server.
Enable FortiClient SSO Mobility Agent service **Enable Authentication**	Select both options to enable single sign-on by clients running FortiClient Endpoint Security. Enter the **Secret key**. Be sure to use the same secret key in the FortiClient Single Sign-On Mobility Agent settings.

5. Select **OK**.

For more information, see the FortiAuthenticator Administration Guide.

Configuring the FortiGate unit

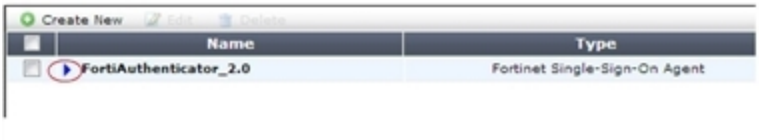
Adding a FortiAuthenticator unit as an SSO agent

On the FortiGate unit, you need to add the FortiAuthenticator unit as a Single Sign-On agent that provides user logon information.

To add a FortiAuthenticator unit as SSO agent:

1. Go to **User & Device > Authentication > Single Sign-On** and select **Create New**.
2. In **Type**, select **Fortinet Single-Sign-On Agent**.
3. Enter a **Name** for the FortiAuthenticator unit.
4. In Primary Agent IP/Name, enter the IP address of the FortiAuthenticator unit.
5. In Password, enter the secret key that you defined for the FortiAuthenticator unit.
   On the FortiAuthenticator unit, you go to **Fortinet SSO Methods > SSO > General** to define the secret key. Select **Enable Authentication**.
6. Select **OK**.

In a few minutes, the FortiGate unit receives a list of user groups from the FortiAuthenticator unit. The entry in the Single Sign-On server list shows a blue caret.



When you open the server, you can see the list of groups. You can use the groups in identity-based security policies.

Configuring an FSSO user group

You cannot use FortiAuthenticator SSO user groups directly in a security policy. Create an FSSO user group and add FortiAuthenticator SSO user groups to it. FortiGate FSSO user groups are available for selection in identity-based security policies.

To create an FSSO user group:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter a **Name** for the group.
3. In Type, select **Fortinet Single Sign-On (FSSO)**.
4. Add **Members**.
   The groups available to add as members are SSO groups provided by SSO agents.
5. Select **OK**.

Configuring security policies

You can create identity-based policies based on FSSO groups as you do for local user groups. For more information about security policies see the Firewall chapter.

Configuring the FortiClient SSO Mobility Agent

The user's device must have at least FortiClient Endpoint Security v5.0 installed. Only two pieces of information are required to set up the SSO Mobility Agent feature: the FortiAuthenticator unit IP address and the preshared secret.

The user needs to know the FortiAuthenticator IP address and preshared secret to set up the SSO Mobility Agent. Or, you could preconfigure FortiClient.

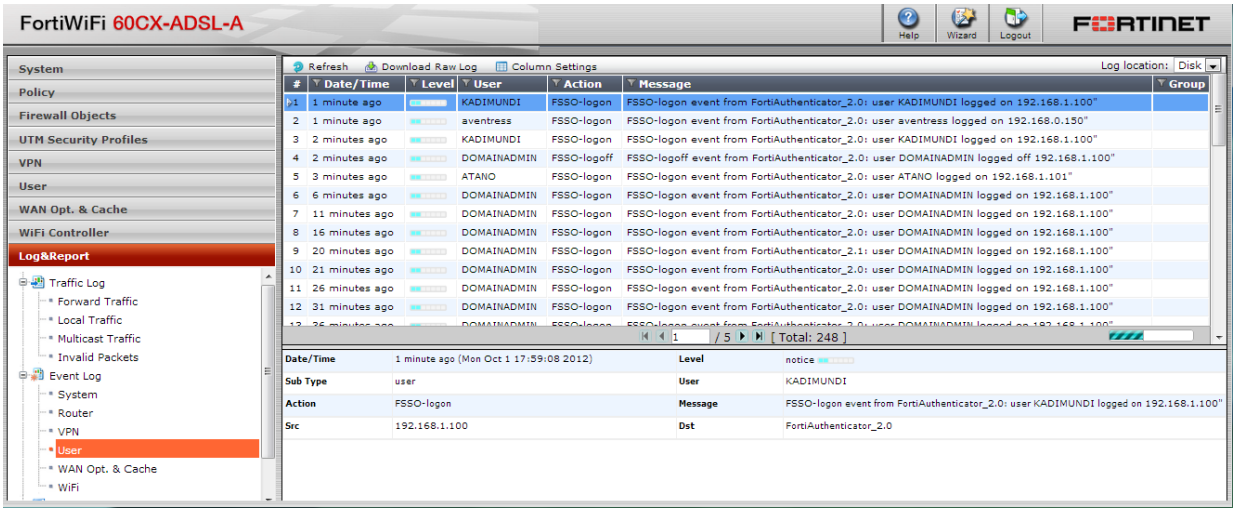
To configure FortiClient SSO Mobility Agent:

1. In FortiClient Endpoint Security, go to **File > Settings**.
   You must run the FortiClient application as an administrator to access these settings.
2. Select **Enable single sign-on mobility agent**. Enter the FortiAuthenticator unit IP address, including the listening port number specified on the FortiAuthenticator unit.
   Example: 192.168.0.99:8001. You can omit the port number if it is 8005.
3. Enter the preshared key.
4. Select **OK**.

Viewing SSO authentication events on the FortiGate unit

User authentication events are logged in the FortiGate event log.

Go to **Log & Report > Event Log > User**.



Single Sign-On to Windows AD

The FortiGate unit can authenticate users transparently and allow them network access based on their privileges in Windows AD. This means that users who have logged on to the network are not asked again for their credentials to access network resources through the FortiGate unit, hence the term “Single Sign-On”.

The following topics are included:

Introduction to Single Sign-On with Windows AD

Introduced in FortiOS 5.0, Single Sign-On (SSO) support provided by FortiGate polling of domain controllers is simpler than the earlier method that relies on agent software installed on Windows AD network servers. No Fortinet software needs to be installed on the Windows network. The FortiGate unit needs access only to the Windows AD global catalog and event log.

When a Windows AD user logs on at a workstation in a monitored domain, the FortiGate unit

- detects the logon event in the domain controller’s event log and records the workstation name, domain, and user,
- resolves the workstation name to an IP address,
- uses the domain controller’s LDAP server to determine which groups the user belongs to,
- creates one or more log entries on the FortiGate unit for this logon event as appropriate.

When the user tries to access network resources, the FortiGate unit selects the appropriate security policy for the destination. The selection consist of matching the FSSO group or groups the user belongs to with the security policy or policies that match that group. If the user belongs to one of the permitted user groups associated with that policy, the connection is allowed. Otherwise the connection is denied.

Configuring Single Sign On to Windows AD

On the FortiGate unit, security policies control access to network resources based on user groups. With Fortinet Single Sign On, this is also true but each FortiGate user group is associated with one or more Windows AD user groups. This is how Windows AD user groups get authenticated in the FortiGate security policy.

Fortinet Single Sign On sends information about Windows user logons to FortiGate units. If there are many users on your Windows AD domains, the large amount of information might affect the performance of the FortiGate unit.

To configure your FortiGate unit to operate with either a Windows AD or a Novell eDirectory FSSO install, you

- Configure LDAP access to the Windows AD global catalog. See Configuring LDAP server access on page 119.
- Configure the LDAP Server as a Single Sign-On server. See Configuring the LDAP Server as a Single Sign-On server on page 120.
- Add Active Directory user groups to FortiGate FSSO user groups. See Creating Fortinet Single Sign-On (FSSO) user groups on page 121.
- Create security policies for FSSO-authenticated groups. See Creating security policies on page 121.
- Optionally, specify a guest protection profile to allow guest access. See Enabling guest access through FSSO security policies on page 123

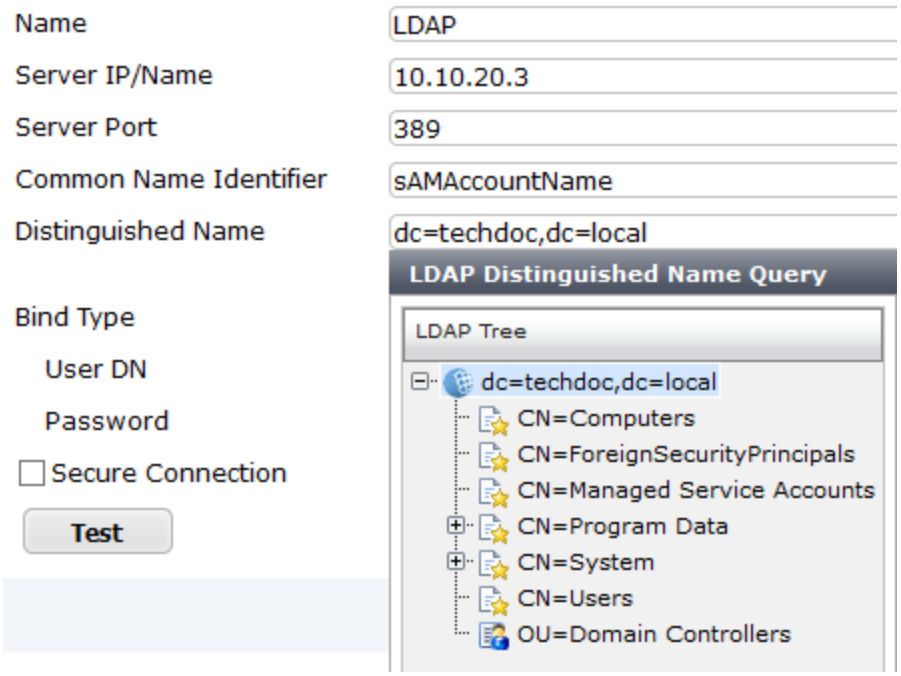
Configuring LDAP server access

The FortiGate unit needs access to the domain controller's LDAP server to retrieve user group information.

The LDAP configuration on the FortiGate unit not only provides access to the LDAP server, it sets up the retrieval of Windows AD user groups for you to select in FSSO. The LDAP Server configuration (in **User & Device > Authentication > LDAP Servers**) includes a function to preview the LDAP server's response to your distinguished name query. If you already know the appropriate Distinguished Name (DN) and User DN settings, you may be able to skip some of the following steps.

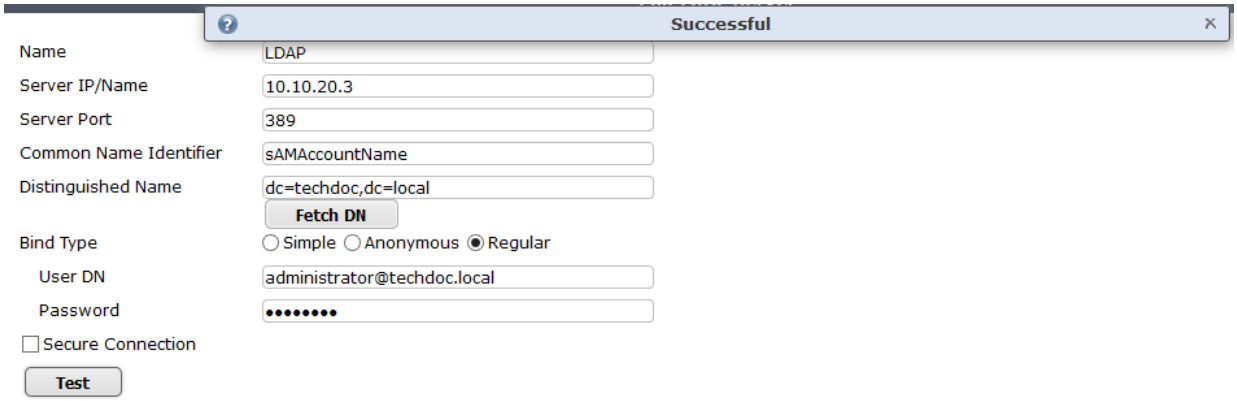
To add an LDAP server - web-based manager:

1. Go to **User & Device > Authentication > LDAP Servers** and select **Create New**.
2. Enter the **Server IP/Name** and **Server Port** (default 389).
3. In the **Common Name Identifier** field, enter **sAMAccountName**.The default common name identifier is `cn`. This is correct for most LDAP servers. However some servers use other identifiers such as `uid`.
4. In the **Distinguished Name** field, enter your organization distinguished name. In this example, Distinguished Name is dc=techdoc,dc=local
5. Select **Fetch DN**, this will fetch the Windows AD directory.



6. Set **Bind Type** to **Regular.**
7. In the **User DN** field, enter the administrative account name that you created for FSSO.
   For example, if the account is administrator, enter “administrator@techdoc.local”.
8. Enter the administrative account password in the **Password** field.
9. Optionally select **Secure Connection**.
   - In the **Protocol** field, select **LDAPS** or **STARTTLS**.
   - In the **Certificate** field, select the appropriate certificate for authentication.

   Note that you need to configure the Windows AD for secure connection accordingly.
10. Select **OK**.
11. Test your configuration by selecting the **Test** button. A successful message confirming the right settings appears.



To configure LDAP for FSSO - CLI example:

```
config user ldap
   edit LDAP
      set server 10.10.20.3
      set cnid sAMAccountName
      set dn dc=techdoc,dc=local
      set type regular
      set username administrator@techdoc.local
      set password <your_password>
   next
end
```

Configuring the LDAP Server as a Single Sign-On server

The LDAP server must be added to the FortiGate Single Sign-On configuration.

To add the LDAP server as a Single Sign-On server:

1. Go to **User & Device > Authentication > Single Sign-On** and select **Create New**.
2. Enter

Type	Poll Active Directory Server
Server IP/Name	Server Name or IP address of the Domain Controller

User	A Domain user name
Password	The user's password
LDAP Server	Select the LDAP server you added earlier.
Enable Polling	Select

3. Select **OK**.

Creating Fortinet Single Sign-On (FSSO) user groups

You cannot use Windows or Novell groups directly in FortiGate security policies. You must create FortiGate user groups of the FSSO type and add Windows or Novell groups to them.

To create a user group for FSSO authentication - web-based manager:

1. Go to **User & Device > User > User Groups** and select **Create New**.
   The **New User Group** dialog box opens.
2. In the **Name** box, enter a name for the group, FSSO_Internet_users for example.
3. In **Type**, select **Fortinet Single Sign-On (FSSO)**.
4. In **Members**, select the required **FSSO** groups.
5. Select **OK**.

To create the FSSO_Internet-users user group - CLI

```
config user group
   edit FSSO_Internet_users
      set group-type fsso-service
      set member CN=Engineering,cn=users,dc=office,dc=example,dc=com
          CN=Sales,cn=users,dc=office,dc=example,dc=com
   end
```

Default FSSO group

`SSO_Guest_users` is a default user group enabled when FSSO is configured. It allows guest users on the network who do not have an FSSO account to authenticate and have access to network resources. See Enabling guest access through FSSO security policies on page 123.

Creating security policies

Policies that require FSSO authentication are very similar to other security policies. Using identity-based policies, you can configure access that depends on the FSSO user group. This allows each FSSO user group to have its own level of access to its own group of services

In this situation, Example.com is a company that has its employees and authentication servers on an internal network. The FortiGate unit intercepts all traffic leaving the internal network and requires FSSO authentication to access network resources on the Internet. The following procedure configures the security policy for FSSO authentication. FSSO is installed and configured including the RADIUS server, FSSO Collector agent, and user groups on the FortiGate

For the following procedure, the internal interface is `port1` and the external interface connected to the Internet is `port2`. There is an address group for the internal network called `company_network`. The FSSO user group is called `fsso_group`, and the FSSO RADIUS server is `fsso_rad_server`.

To configure an FSSO authentication security policy - web-based manager:

1. Go to **Policy & Objects > Policy > IP4** and select **Create New**.
2. Enter the following information.

Incoming Interface	port1
Source Address	company_network
Source User(s)	`fsso_group`
Outgoing Interface	port2
Destination Address	all
Schedule	always
Service	HTTP, HTTPS, FTP, and Telnet
Action	ACCEPT
NAT	ON
UTM Security Profiles	ON for AntiVirus, IPS, Web Filter, and Email Filter, all using default profiles.
Log Allowed Traffic	ON. Select **Security Events**.

3. Select **OK**.
4. Ensure the FSSO authentication policy is higher in the policy list than more general policies for the same interfaces.

To create a security policy for FSSO authentication - CLI:

```
config firewall policy
   edit 0
      set srcintf port1
      set dstintf port2
      set srcaddr company_network
      set dstaddr all
      set action accept
      set groups fsso_group
      set schedule always
      set service HTTP HTTPS FTP TELNET
      set nat enable
   end
```

Here is an example of how this FSSO authentication policy is used. Example.com employee on the internal company network logs on to the internal network using their RADIUS username and password. When that user attempts to access the Internet, which requires FSSO authentication, the FortiGate authentication security policy

intercepts the session, checks with the FSSO Collector agent to verify the user's identity and credentials, and then if everything is verified the user is allowed access to the Internet.

Enabling guest access through FSSO security policies

You can enable guest users to access FSSO security policies. Guests are users who are unknown to Windows AD and servers that do not logon to a Windows AD domain.

To enable guest access in your FSSO security policy, add an identity-based policy assigned to the built-in user group `SSO_Guest_Users`. Specify the services, schedule and UTM profiles that apply to guest users — typically guests have access to a reduced set of services. See Creating security policies on page 121.

FortiOS FSSO log messages

There are two types of FortiOS log messages — firewall and event. FSSO related log messages are generated from authentication events. These include user logon and log off events, and NTLM authentication events. These log messages are central to network accounting policies, and can also be useful in troubleshooting issues. For more information on firewall logging, see Enabling security logging on page 79. For more information on logging, see the FortiOS Handbook Logging and Reporting guide.

Enabling authentication event logging

For the FortiGate unit to log events, that specific type of event must be enabled under logging.

When VDOMs are enabled certain options may not be available, such as CPU and memory usage events. You can enable event logs only when you are logged on to a VDOM; you cannot enable event logs globally.

To ensure you log all the events needed, set the minimum log level to Notification or Information. Firewall logging requires Notification as a minimum. The closer to Debug level, the more information will be logged.

To enable event logging:

1. Go to **Log&Report > Log Config > Log Settings**.
2. In **Event Logging**, select

System activity event	All system-related events, such as ping server failure and gateway status.
User activity event	All administration events, such as user logins, resets, and configuration updates.

3. Select **Apply**.

List of FSSO related log messages

Message ID	Severity	Description
43008	Notification	Authentication was successful
43009	Notification	Authentication session failed

Message ID	Severity	Description
43010	Warning	Authentication locked out
43011	Notification	Authentication timed out
43012	Notification	FSSO authentication was successful
43013	Notification	FSSO authentication failed
43014	Notification	FSSO user logged on
43015	Notification	FSSO user logged off
43016	Notification	NTLM authentication was successful
43017	Notification	NTLM authentication failed

For more information on logging, see the FortiOS Handbook Logging and Reporting guide.

Testing FSSO

Once FSSO is configured, you can easily test to ensure your configuration is working as expected. For additional FSSO testing, see Troubleshooting FSSO on page 124.

1. Logon to one of the stations on the FSSO domain, and access an Internet resource.
2. Connect to the CLI of the FortiGate unit, and if possible log the output.
3. Enter the following command:`diagnose debug authd fsso list`
4. Check the output. If FSSO is functioning properly you will see something similar to the following:

```
----FSSO logons----
IP: 192.168.1.230 User: ADMINISTRATOR Groups: VLAD-AD/DOMAIN USERS
IP: 192.168.1.240 User: ADMINISTRATOR Groups: VLAD-AD/DOMAIN USERS
Total number of users logged on: 2
----end of FSSO logons----
```

   The exact information will vary based on your installation.

5. Check the FortiGate event log, for FSSO-auth action or other FSSO related events with FSSO information in the message field.
6. To check server connectivity, run the following commands from the CLI:

```
FGT# diagnose debug enable
FGT# diagnose debug authd fsso server-status
FGT# Server Name Connection Status
     ----------- -----------------
     SBS-2003 connected
```

Troubleshooting FSSO

When installing, configuring, and working with FSSO some problems are quite common. A selection of these problems follows including explanations and solutions.

Some common Windows AD problems include:

General troubleshooting tips for FSSO

The following tips are useful in many FSSO troubleshooting situations.

- Ensure all firewalls are allowing the FSSO required ports through.
  FSSO has a number of required ports that must be allowed through all firewalls or connections will fail. These include: ports 139, 389 (LDAP), 445, 636 (LDAP).
- Ensure there is at least 64kbps bandwidth between the FortiGate unit and domain controllers. If there is insufficient bandwidth, some FSSO information might not reach the FortiGate unit. The best solution is to configure traffic shaping between the FortiGate unit and the domain controllers to ensure that the minimum bandwidth is always available.

Users on a particular computer (IP address) can not access the network

Windows AD Domain Controller agent gets the username and workstation where the logon attempt is coming from. If there are two computers with the same IP address and the same user trying to logon, it is possible for the authentication system to become confused and believe that the user on computer_1 is actually trying to access computer_2.

Windows AD does not track when a user logs out. It is possible that a user logs out on one computer, and immediate logs onto a second computer while the system still believes the user is logged on the original computer. While this is allowed, information that is intended for the session on one computer may mistakenly end up going to the other computer instead. The result would look similar to a hijacked session.

Solutions

- Ensure each computer has separate IP addresses.
- Encourage users to logout on one machine before logging onto another machine.
- If multiple users have the same username, change the usernames to be unique.
- Shorten timeout timer to flush inactive sessions after a shorter time.

Guest users do not have access to network

A group of guest users was created, but they don’t have access.

Solution

The group of the guest users was not included in a policy, so they do not fall under the guest account. To give them access, associate their group with a security policy.

Additionally, there is a default group called `SSO_Guest_Users`. Ensure that group is part of an identity-based security policy to allow traffic.

Agent-based FSSO

FortiOS can provide single sign-on capabilities to Windows AD, Citrix, or Novell eDirectory users with the help of agent software installed on these networks. The agent software sends information about user logons to the FortiGate unit. With user information such as IP address and user group memberships from the network, FortiGate security policies can allow authenticated network access to users who belong to the appropriate user groups without requesting their credentials again.

For Windows AD networks, FortiGate units can provide SSO capability without agent software by directly polling the Windows AD domain controllers. For information about this type of SSO, seeSingle Sign-On to Windows AD on page 118.

The following topics are included:

Introduction to agent-based FSSO

Fortinet Single Sign-On (FSSO), through agents installed on the network, monitors user logons and passes that information to the FortiGate unit. When a user logs on at a workstation in a monitored domain, FSSO

- detects the logon event and records the workstation name, domain, and user,
- resolves the workstation name to an IP address,
- determines which user groups the user belongs to,
- sends the user logon information, including IP address and groups list, to the FortiGate unit
- creates one or more log entries on the FortiGate unit for this logon event as appropriate.

When the user tries to access network resources, the FortiGate unit selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups associated with that policy, the connection is allowed. Otherwise the connection is denied.

FSSO can also provide NTLM authentication service for requests coming from FortiGate. SSO is very convenient for users, but may not be supported across all platforms. NTLM is not as convenient, but it enjoys wider support. See FSSO NTLM authentication support on page 132.

Introduction to FSSO agents

There are several different FSSO agents that can be used in an FSSO implementation:

- Domain Controller (DC) agent
- eDirectory agent
- Citrix/Terminal Server (TS) agent
- Collector (CA) agent

Consult the latest FortiOS and FSSO Release Notes for operating system compatibility information.

Domain Controller (DC) agent

The Domain Controller (DC) agent must be installed on every domain controller if you will use DC Agent mode, but is not required if you use Polling mode. See FSSO for Windows AD on page 128.

eDirectory agent

The eDirectory agent is installed on a Novell network to monitor user logons and send the required information to the FortiGate unit. It functions much like the Collector agent on a Windows AD domain controller.The agent can obtain information from the Novell eDirectory using either the Novell API or LDAP.

Citrix/Terminal Server (TS) agent

The Citrix/Terminal Server (TS) agent is installed on a Citrix terminal server to monitor user logons in real time. It functions much like the DC Agent on a Windows AD domain controller.

Collector (CA) agent

This agent is installed as a service on a server in the Windows AD network to monitor user logons and send the required information to the FortiGate unit. The Collector agent can collect information from

- Domain Controller agent (Windows AD)
- TS agent (Citrix Terminal Server)

In a Windows AD network, the Collector agent can optionally obtain logon information by polling the AD domain controllers. In this case, DC agents are not needed.

The Collector can obtain user group information from the DC agent or optionally, a FortiGate unit can obtain group information directly from AD using Lightweight Directory Access Protocol (LDAP).

On a Windows AD network, the FSSO software can also serve NT LAN Manager (NTLM) requests coming from client browsers (forwarded by the FortiGate unit) with only one or more Collector agents installed. See FSSO NTLM authentication support on page 132.

The CA is responsible for DNS lookups, group verification, workstation checks, and as mentioned FortiGate updates of logon records. The FSSO Collector Agent sends Domain Local Security Group and Global Security Group information to FortiGate units. The CA communicates with the FortiGate over TCP port 8000 and it listens on UDP port 8002 for updates from the DC agents.

The FortiGate unit can have up to five CAs configured for redundancy. If the first on the list is unreachable, the next is attempted, and so on down the list until one is contacted. See Configuring FSSO on FortiGate units on page 159.

All DC agents must point to the correct Collector agent port number and IP address on domains with multiple DCs.

A FortiAuthenticator unit can act much like a Collector agent, collecting Windows AD user logon information and sending it to the FortiGate unit. It is particularly useful in large installations with several FortiGate units. For more information, see the FortiAuthenticator Administration Guide.

FSSO for Windows AD

FSSO for Windows AD requires at least one Collector agent. Domain Controller agents may also be required depending on the Collector agent working mode. There are two working modes to monitor user logon activity: DC Agent mode or Polling mode.

Collector agent DC Agent mode versus Polling mode

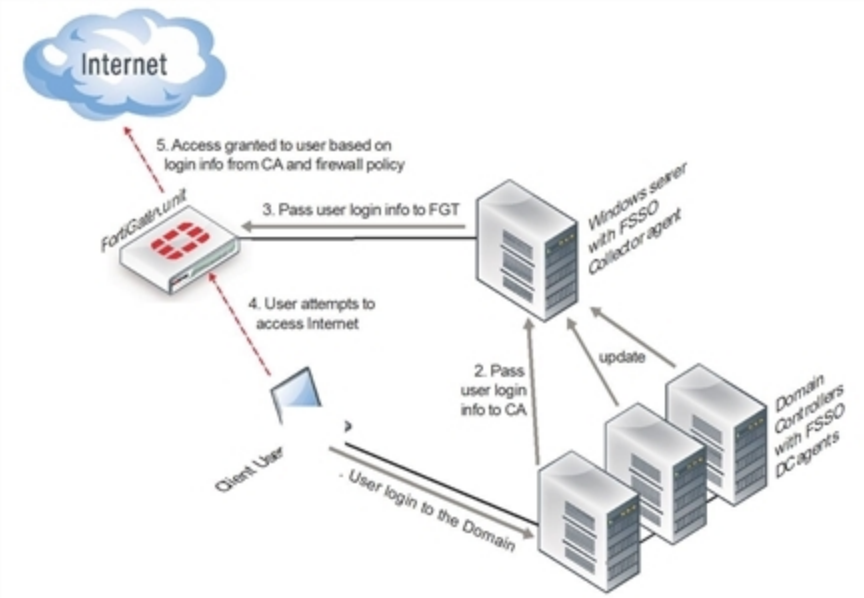
	DC Agent mode	Polling Mode
Installation	Complex — Multiple installations: one agent per DC plus Collector agent, requires a reboot	Easy — Only Collector agent installation, no reboot required
Resources	Shares resources with DC system	Has own resources
Network load	Each DC agent requires minimum 64kpbs bandwidth, adding to network load	Increase polling period during busy period to reduce network load
Level of Confidence	Captures all logons	Potential to miss a login if polling period is too great

DC Agent mode

DC Agent mode is the standard mode for FSSO. In DC Agent mode, a Fortinet authentication agent is installed on each domain controller. These DC agents monitor user logon events and pass the information to the Collector agent, which stores the information and sends it to the FortiGate unit.

The DC agent installed on the domain controllers is not a service like the Collector agent — it is a DLL file called `dcagent.dll` and is installed in the `Windows\system32` directory. It must be installed on all domain controllers of the domains that are being monitored.

FSSO in DC agent mode



DC Agent mode provides reliable user logon information, however you must install a DC agent on every domain controller. A reboot is needed after the agent is installed. Each installation requires some maintenance as well. For these reasons it may not be possible to use the DC Agent mode.

Each domain controller connection needs a minimum guaranteed 64kpbs bandwidth to ensure proper FSSO functionality. You can optionally configure traffic shapers on the FortiGate unit to ensure this minimum bandwidth is guaranteed for the domain controller connections.

Polling mode

In Polling mode there are three options — NetAPI polling, Event log polling, and Event log using WMI. All share the advantages of being transparent and agentless.

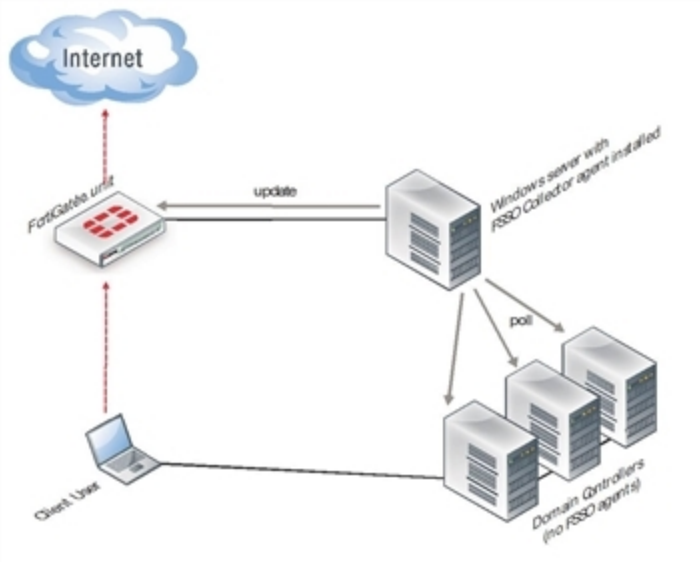
NetAPI polling is used to retrieve server logon sessions. This includes the logon event information for the Controller agent. NetAPI runs faster than Event log polling but it may miss some user logon events under heavy system load. It requires a query round trip time of less than 10 seconds.

Event log polling may run a bit slower, but will not miss events, even when the installation site has many users that require authentication. It does not have the 10 second limit on NetAPI polling. Event log polling requires fast network links. Event log polling is required if there are Mac OS users logging into Windows AD.

Event log using WMI polling: WMI is a Windows API to get system information from a Windows server, CA is a WMI client and sends WMI queries for user logon events to DC, which in this case is a WMI server. Main advantage in this mode is that CA does not need to search security event logs on DC for user logon events, instead, DC returns all requested logon events via WMI. This also reduces network load between CA and DC.

In Polling mode, the Collector agent polls port 445 of each domain controller for user logon information every few seconds and forwards it to the FortiGate unit. There are no DC Agents installed, so the Collector agent polls the domain controllers directly.

FSSO in Polling mode



A major benefit of Polling mode is that no FSSO DC Agents are required. If it is not possible to install FSSO DC Agents on your domain controllers, this is the alternate configuration available to you. Polling mode results in a less complex install, and reduces ongoing maintenance. The minimum permissions required in Polling mode are to read the event log or call NetAPI.

Collector agent AD Access mode - Standard versus Advanced

The Collector agent has two ways to access Active Directory user information. The main difference between Standard and Advanced mode is the naming convention used when referring to username information.

Standard mode uses regular Windows convention: Domain\Username. Advanced mode uses LDAP convention: CN=User, OU=Name, DC=Domain.

If there is no special requirement to use LDAP— best practices suggest you set up FSSO in Standard mode. This mode is easier to set up, and is usually easier to maintain and troubleshoot.

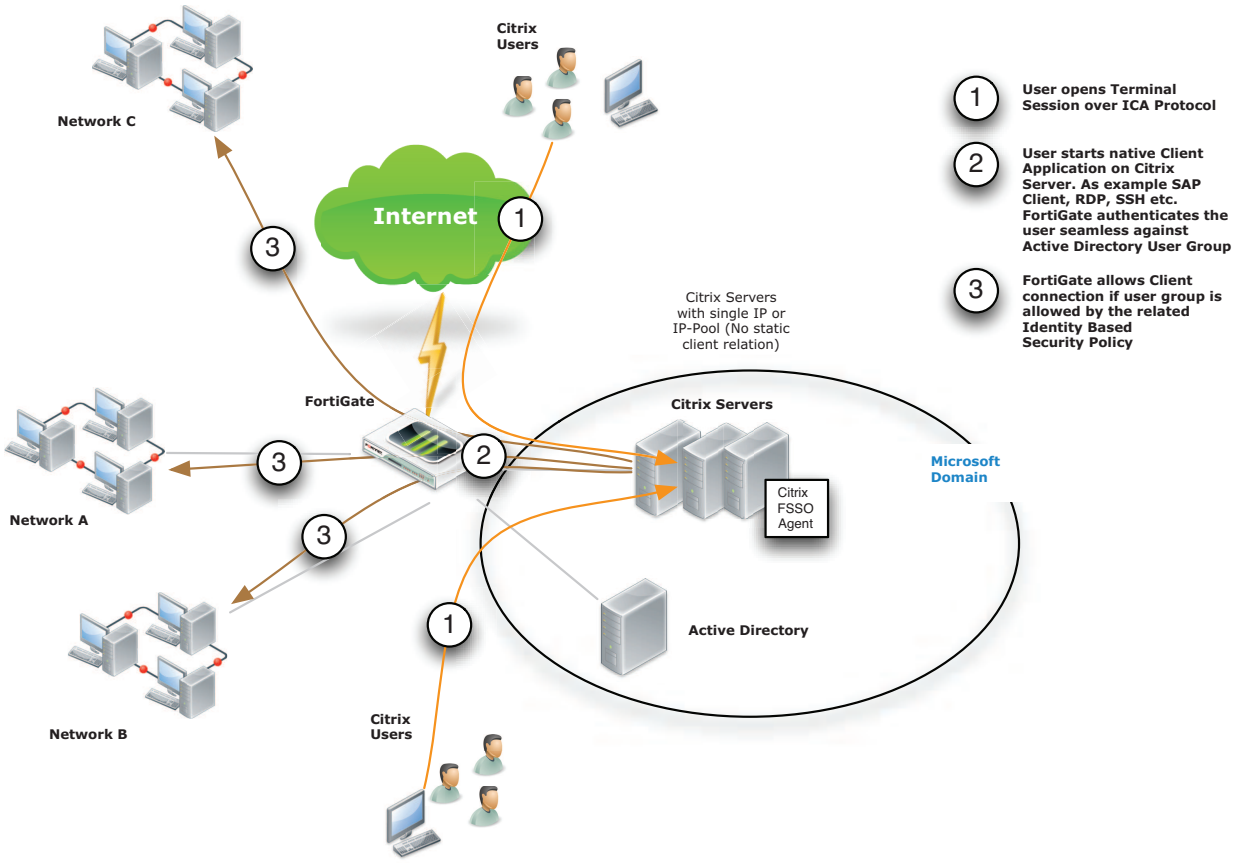
Standard and advanced modes have the same level of functionality with the following exceptions:

- Users have to create Group filters on the Collector agent. This differs from Advanced mode where Group filters are configured from the FortiGate unit. Fortinet strongly encourages users to create filters from CA.
- Advanced mode supports nested or inherited groups. This means that users may be a member of multiple monitored groups. Standard mode does not support nested groups so a user must be a direct member of the group being monitored.

FSSO for Citrix

Citrix users can enjoy a similar Single Sign-On experience as Windows AD users. The FSSO TS agent installed on each Citrix server provides user logon information to the FSSO Collector agent on the network. The FortiGate unit uses this information to authenticate the user in security policies.

Citrix SSO topology



Citrix users do not have unique IP addresses. When a Citrix user logs on, the TS agent assigns that user a range of ports. By default each user has a range of 200 ports.

FSSO for Novell eDirectory

FSSO in a Novell eDirectory environment works similar to the FSSO Polling mode in the Windows AD environment. The eDirectory agent polls the eDirectory servers for user logon information and forwards the information to the FortiGate unit. There is no need for the Collector agent.

When a user logs on at a workstation, FSSO:

- detects the logon event by polling the eDirectory server and records the IP address and user ID,
- looks up in the eDirectory which groups this user belongs to,
- sends the IP address and user groups information to the FortiGate unit.

When the user tries to access network resources, the FortiGate unit selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

FSSO is supported on the Novell E-Directory 8.8 operating system.

For a Novell network, there is only one FSSO component to install — the eDirectory agent. In some cases, you also need to install the Novell Client.

FSSO security issues

When the different components of FSSO are communicating there are some inherent security features.

FSSO installation requires an account with network admin privileges. The security inherent in these types of accounts helps ensure access to FSSO configurations is not tampered with.

User passwords are never sent between FSSO components. The information that is sent is information to identify a user including the username, group or groups, and IP address.

NTLM uses base-64 encoded packets, and uses a unique randomly generated challenge nonce to avoid sending user information and password between the client and the server.

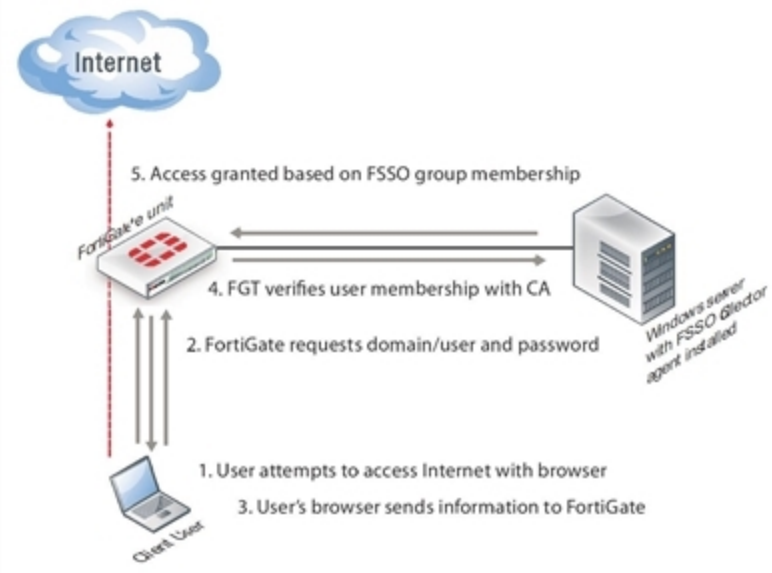
FSSO NTLM authentication support

In a Windows AD network, FSSO can also provide NTLM authentication service to the FortiGate unit. When the user makes a request that requires authentication, the FortiGate unit initiates NTLM negotiation with the client browser. The FortiGate unit does not process the NTLM packets itself. Instead, it forwards all the NTLM packets to the FSSO service to process.

NTLM has the benefit of not requiring an FSSO agent, but it is not transparent to users, and the user's web browser must support NTLM.

The NTLM protocol protects the user's password by not sending it over the network. Instead, the server sends the client a random number that the client must encrypt with the hash value of the user's password. The server compares the result of the client's encryption with the result of its own encryption. The two will match only if both parties used the same password.

NTLM authentication



If the NTLM authentication with the Windows AD network is successful, and the user belongs to one of the groups permitted in the applicable security policy, the FortiGate unit allows the connection but will require authentication again in the future when the current authentication expires.

Fortinet has tested NTLM authentication with Internet Explorer and Firefox browsers.

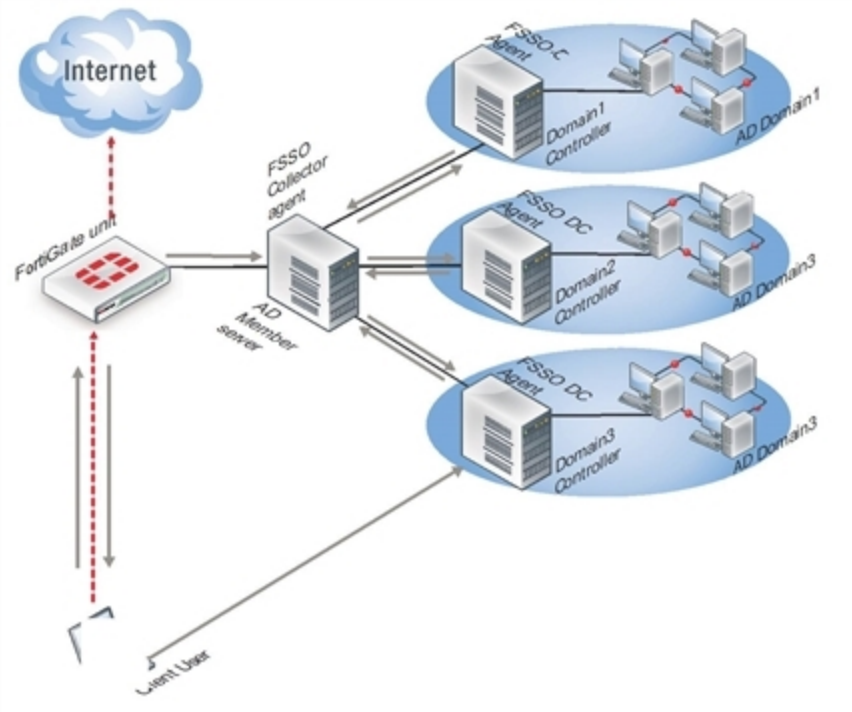
NTLM in a multiple domain environment

In a multiple domain environment for NTLM, the important factor is that there is a trust relation between the domains. In a forest, this relation is automatically created. So you can install FSSO agent on one of the domain controllers without worry.

But in case of multiple domains that are not in a forest, you need to create a trust relation between the domains. If you do not want to have a trust relation between your multiple domains, you need to use FSAE 4.0 MR1 and the DC agent needs to be installed once on each domain. Then you can use security policies to configure server access.

In the figure below, three domains are shown connected to the FSSO Collector agent server. The Client logs on to their local Domain Controller, which then sends the user logon event information to the Collector Agent. When the Client attempts to access the Internet, the FortiGate unit contacts the Collector Agent for the logon information, sees the Client is authenticated, and allows access to the Internet. There are multiple domains each with a domain controller agent (DCagent) that sends logon information to the Collector agent. If the multiple domains have a trust relationship, only one DCagent is required instead of one per domain.

FSSO NTLM with multiple domains not in a forest



Understanding the NTLM authentication process

1. The user attempts to connect to an external (internet) HTTP resource. The client application (browser) on the user's computer issues an unauthenticated request through the FortiGate unit.

2. The FortiGate is aware that this client has not authenticated previously, so responds with a `401 Unauthenticated` status code, and tells the client which authentication method to reply with in the header: `Proxy-Authenticated: NTLM`. Then the initial session is dismantled.
3. The client application connects again to the FortiGate, and issues a GET-request, with a `Proxy-Authorization: NTLM <negotiate string>` header. `<negotiate-string>` is a base64-encoded NTLM Type 1 negotiation packet.
4. The FortiGate unit replies with a `401 "proxy auth required"` status code, and a `Proxy-Authenticate: NTLM <challenge string>` (a base 64-encoded NTLM Type 2 challenge packet). In this packet is the challenge nonce, a random number chosen for this negotiation that is used once and prevents replay attacks.

The TCP connection must be kept alive, as all subsequent authentication-related information is tied to the TCP connection. If it is dropped, the authentication process must start again from the beginning.

5. The client sends a new GET-request with a header: `Proxy-Authenticate: NTLM <authenticate string>`, where `<authenticate string>` is a NTLM Type 3 Authentication packet that contains:
   - username and domain
   - the challenge nonce encoded with the client password (it may contain the challenge nonce twice using different algorithms).
6. If the negotiation is successful and the user belongs to one of the groups permitted in the security policy, the connection is allowed, Otherwise, the FortiGate unit denies the authentication by issuing a 401 return code and prompts for a username and password. Unless the TCP connection is broken, no further credentials are sent from the client to the proxy.

If the authentication policy reaches the authentication timeout period, a new NTLM handshake occurs.

Agent installation

After reading the appropriate sections of Introduction to agent-based FSSO on page 126 to determine which FSSO agents you need, you can proceed to perform the necessary installations.

Ensure you have administrative rights on the servers where you are installing FSSO agents. It is best practice to install FSSO agents using the built-in local administrator account. Optionally, you can install FSSO without an admin account. See Installing FSSO without using an administrator account on page 137.

In Windows 2008 by default, you do not have administrative user rights if you are logged on as a user other than as the built-in administrator, even if you were added to the local Administrators group on the computer.

The FSSO installer first installs the Collector agent. You can then continue with installation of the DC agent, or you can install it later by going to **Start > Programs > Fortinet > Fortinet Single Sign On Agent > Install DC Agent**. The installer will install a DC agent on the domain controllers of all of the trusted domains in your network.

Each domain controller connection needs a minimum guaranteed 64kpbs bandwidth to ensure proper FSSO functionality.Traffic shapers configured on the FortiGate can help guarantee these minimum bandwidths.

Collector agent installation

To install FSSO, you must obtain the FSSO_Setup file from the Fortinet Support web site. This is available as either an executable (.exe) or a Microsoft Installer (.msi) file. Then you follow these two installation procedures on the server that will run the Collector agent. This can be any server or domain controller that is part of your network. These procedures also installs the DC Agent on all of the domain controllers in your network.

To install the Collector agent:

1. Create an account with administrator privileges and a password that does not expire. See Microsoft Advanced Server documentation for help with this task.
   To use a non-admin read only account, see Installing FSSO without using an administrator account on page 137.
2. Log on to the account that you created in Step 1.
3. Double-click the `FSSOSetup.exe` file.
   The Fortinet SSO Collector Agent Setup Wizard starts.
4. Select **Next**.
5. Read and accept the license agreement. Select **Next**.
6. Optionally, you can change the installation location. Select **Next**.
7. Optionally, change the **User Name**.
8. By default, the agent is installed using the currently running account. If you want FSSO to use another existing admin account, change the **User Name** using the format DomainName \ UserName. For example if the account is `jsmith` and the domain is **example_corp** you would enter `example_corp\jsmith`.
9. In the **Password** field, enter the password for the account listed in the **User Name** field.
10. Select **Next**.
11. Enable as needed:
    - Monitor user logon events and send the information to the FortiGate unit
    - Serve NTLM authentication requests coming from FortiGate
      By default, both methods are enabled. You can change these options after installation.
12. Select the access method to use for Windows Directory:
13. Select **Standard** to use Windows domain and username credentials.
14. Select **Advanced** if you will set up LDAP access to Windows Directory.
    See Collector agent AD Access mode - Standard versus Advanced on page 130.
15. Select **Next** and then select **Install**.
    If you want to use DC Agent mode, ensure that **Launch DC Agent Install Wizard** is selected. This will start DC agent installation immediately after you select **Finish**.
16. Select **Finish**.

If you see an error such as Service Fortinet Single Sign On agent (service_FSAE) failed to start, there are two possible reasons for this. Verify the user account you selected has sufficient privileges to run the FSSO service. Also verify the computer system you are attempting to install on is a supported operating system and version.

DC agent installation

The FSSO_Setup file contains both the Collector agent and DC Agent installers, but the DC Agent installer is also available separately as either a .exe or .msi file named DCAgent_Setup.

To install the DC Agent

1. If you have just installed the Collector agent, the FSSO - Install DC Agent wizard starts automatically. Otherwise, go to **Start > Programs > Fortinet > Fortinet Single Sign On Agent > Install DC Agent**.
2. Select **Next**.
3. Read and accept the license agreement. Select **Next**.
4. Optionally, you can change the installation location. Select **Next**.
5. Enter the **Collector agent IP address**.
6. If the Collector agent computer has multiple network interfaces, ensure that the one that is listed is on your network. The listed **Collector agent listening port** is the default. Only change this if the port is already used by another service.
7. Select **Next**.
8. Select the domains to monitor and select **Next**.
9. If any of your required domains are not listed, cancel the wizard and set up the proper trusted relationship with the domain controller. Then run the wizard again by going to **Start > Programs > Fortinet > Fortinet Single Sign On Agent > Install DC Agent**.
10. Optionally, select users that you do not want monitored. These users will not be able to authenticate to FortiGate units using FSSO. You can also do this later. See Configuring the FSSO Collector agent for Windows AD on page 140.
11. Select **Next**.
12. Optionally, clear the check boxes of domain controllers on which you do not want to install the DC Agent.
13. Select the **Working Mode** as DC Agent Mode. While you can select Polling Mode here, in that situation you would not be installing a DC Agent. For more information, see DC Agent mode on page 128 and Polling mode on page 129.
14. Select **Next**.
15. Select **Yes** when the wizard requests that you reboot the computer.

If you reinstall the FSSO software on this computer, your FSSO configuration is replaced with default settings.

If you want to create a redundant configuration, repeat the Collector agent installation procedure on at least one other Windows AD server.

When you start to install a second Collector agent, cancel the Install Wizard dialog appears the second time. From the configuration GUI, the monitored domain controller list will show your domain controllers un-selected. Select the ones you wish to monitor with this Collector agent, and select **Apply**.

Before you can use FSSO, you need to configure it on both Windows AD and on the FortiGate units. Configuring FSSO on FortiGate units on page 159 will help you accomplish these two tasks.

Installing FSSO without using an administrator account

Normally when installing services in Windows, it is best to use the Domain Admin account, as stated earlier. This ensures installation goes smoothly and uninterrupted, and when using the FSSO agent there will be no permissions issues. However, it is possible to install FSSO with a non-admin account in Windows 2003 or 2008 AD.

The following instructions for Windows 2003 are specific to the event log polling mode only. Do not use this procedure with other FSSO configurations.

Windows 2003

There are two methods in Windows 2003 AD for installing FSSO without an admin account — add the non-admin user to the security log list, and use a non-admin account with read-only permissions. A problem with the first method is that full rights (read, write, and clear) are provided to the event log. This can be a problem when audits require limited or no write access to logs. In those situations, the non-admin account with read-only permissions is the solution.

To add the non-admin user account to the Windows 2003 security log list :

1. Go to **Default Domain Controller Security Settings > Security Settings > User Rights Assignment > Manage auditing and security log**.
2. Add the user account to this list.
3. Repeat these steps on every domain controller in Windows 2003 AD.
   A reboot is required.

To use a non-admin account with read-only permissions to install FSSO on Windows 2003:

The following procedure provides the user account specified with read only access to the Windows 2003 AD Domain Controller Security Event Log which allows FSSO to function.

1. Find out the SID of the account you intend to use.
   Tools for this can be downloaded for free from http://technet.microsoft.com/en-us/sysinternals/bb897417.
2. Then create the permission string. For example:
   - `(A;;0x1;;;S-1-5-21-4136056096-764329382-1249792191-1107)`
   - `A` means Allow,
   - `0x1` means Read, and
   - `S-1-5-21-4136056096-764329382-1249792191-1107` is the SID.

3. Then, append it to the registry key:
   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\Security\CustomSD`
4. Repeat these steps on every domain controller in Windows 2003 AD.
   A reboot is required.

Windows 2008

In Windows 2008 AD, if you do not want to use the Domain Admin account then the user account that starts the FSSO agent needs to be added to the Event Log Readers group.

When the user is added to the Event Log Readers group, that user is now allowed to have read only access to the event log and this is the minimal rights required for FSSO to work.

Citrix TS agent installation

To install the Citrix TS agent, you must obtain the TSAgent_Setup file from the Fortinet Support web site. Perform the following installation procedure on the Citrix server.

To install the FSSO TS agent:

1. On the Citrix server, create an account with administrator privileges and a password that does not expire. See Citrix documentation for more information.
2. Log on to the account that you created in step 1.
3. Double-click the TSAgent_Setup installation file.
   The Fortinet SSO Terminal Server Agent Setup Wizard starts.
4. Select **Next**.
5. Read and accept the license agreement. Select **Next**.
6. Optionally, you can change the installation location. Select **Next**.
7. Verify that **This Host IP Address** is correct.
8. In the **FSSO Collector Agent List**, enter the IP address(es) of your Collector Agents.
9. Select **Next** and then select **Install**.
   The TS agent is installed.
10. Select **Finish**.

Novell eDirectory agent installation

To install the eDirectory agent, you must obtain the FSSO_Setup_eDirectory file from the Fortinet Support web site. Perform the following installation procedure on the computer that will run the eDirectory agent. This can be any server or domain controller that is part of your network. You will need to provide some setup information.

To install the FSSO eDirectory agent:

1. Create an account with administrator privileges and a password that does not expire. See Novell documentation for more information.
2. Log on to the account that you created in step 1.
3. Double-click the FSSO_Setup_edirectory file to start the installation wizard.
4. Select **Next**.
5. Read and accept the license agreement. Select **Next**.
6. Optionally, change the installation location. Select **Next**.
7. Enter:

eDirectory Server	
Server Address	Enter the IP address of the eDirectory server.
Use secure connection (SSL)	Select to connect to the eDirectory server using SSL security.
Search Base DN	Enter the base Distinguished Name for the user search.

eDirectory Authentication	
Username	Enter a username that has access to the eDirectory, using LDAP format.
User password	Enter the password.

8. Select **Next**.
9. Select **Install**. When the installation completes, select **Finish**.

Updating FSSO agents on Windows AD

After FSSO is installed on your network, you may want to upgrade to a newer version. The following procedure helps ensure you have a trouble free upgrade. How you update FSSO depends on if you are using polling mode or DCAgent mode.

For polling mode, since there are no DC agents you only need to upgrade the Collector. However in DCAgent mode, each DC Agent must be updated as well.

To update FSSO in DC Agent mode:

1. Go to the system32 directory on all DC's and rename the `dcagent.dll` file to `dcagent.dll.old`. This ensures the when the upgrade is pushed to the DC it does not overwrite the old file. If there are any problems this makes it easy to revert to the old version.
2. Run the FSSO setup .exe file to update the collector. When this is completed, ignore any reboot message.
3. Go to **Programs > Fortinet > Fortinet Single Sign On Agent > Install DC Agent** and push the DC agent out to all servers. All DC's will now need to be rebooted so that the new DLL file is loaded.
4. After the reboot, go to all DC's and delete the `dcagent.dll.old` files.

Configuring the FSSO Collector agent for Windows AD

On the FortiGate unit, security policies control access to network resources based on user groups. With Fortinet Single Sign On, this is also true but each FortiGate user group is associated with one or more Windows AD user groups. This is how Windows AD user groups get authenticated in the FortiGate security policy.

Fortinet Single Sign On sends information about Windows user logons to FortiGate units. If there are many users on your Windows AD domains, the large amount of information might affect the performance of the FortiGate units.

To avoid this problem, you can configure the Fortinet Single Sign On Collector agent to send logon information only for groups named in the FortiGate unit's security policies. See Configuring FortiGate group filters on page 147.

On each server with a Collector agent, you will be

- Configuring Windows AD server user groups
- Configuring Collector agent settings, including the domain controllers to be monitored
- Selecting Domain Controllers and working mode for monitoring
- Configuring Directory Access settings
- Configuring the Ignore User List
- Configuring FortiGate group filters for each FortiGate unit
- Configuring FSSO ports
- Configuring alternate user IP address tracking
- Viewing FSSO component status

Configuring Windows AD server user groups

FortiGate units control network resource access at the group level. All members of a user group have the same network access as defined in FortiGate security policies.

You can use existing Windows AD user groups for authentication to FortiGate units if you intend that all members within each group have the same network access privileges.

Otherwise, you need to create new user groups for this purpose.

If you change a user's group membership, the change does not take effect until the user logs off and then logs on again.

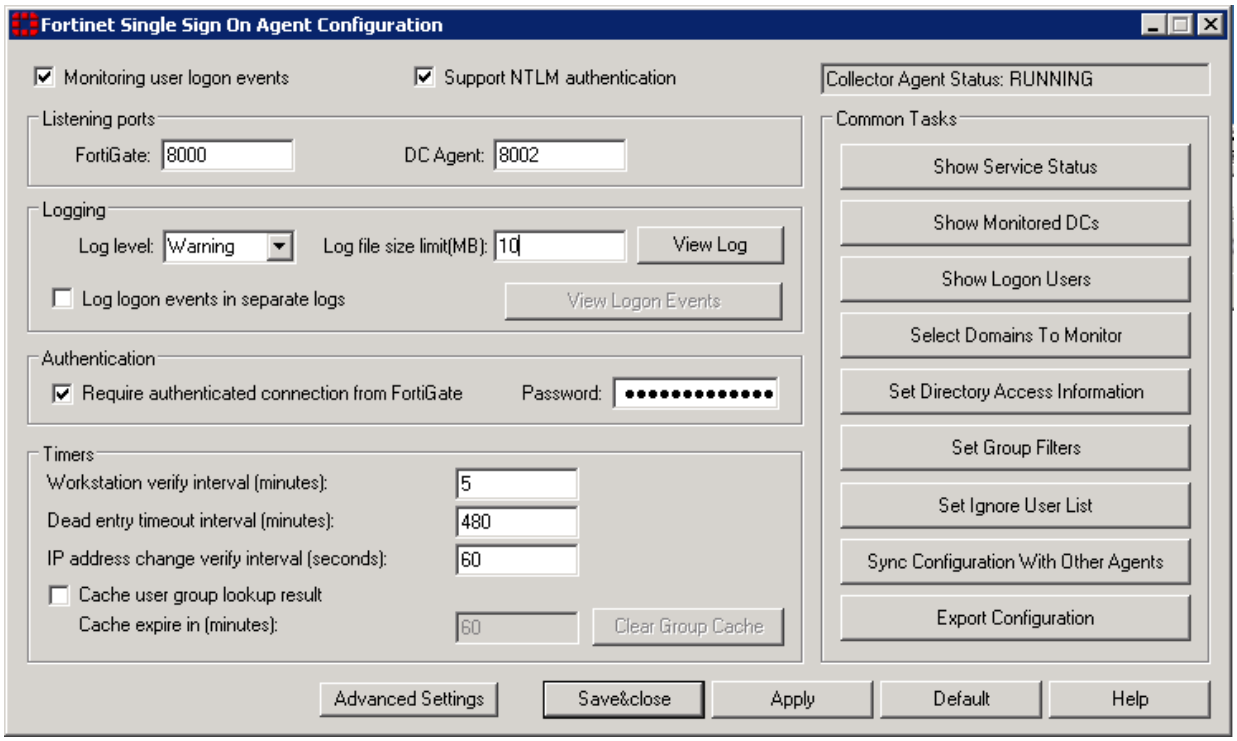
The FSSO Agent sends only Domain Local Security Group and Global Security Group information to FortiGate units. You cannot use Distribution group types for FortiGate access. No information is sent for empty groups.

Refer to Microsoft documentation for information about creating and managing Windows AD user groups.

Configuring Collector agent settings

You need to configure which domain controllers the Collector agent will use and which domains to monitor for user logons. You can also alter default settings and settings you made during installation. These tasks are accomplished by configuring the FSSO Collector Agent, and selecting either Apply to enable the changes.

At any time to refresh the FSSO Agent settings, select Apply.



To configure the Collector agent:

1. From the Start menu, select **Programs > Fortinet > Fortinet Single Sign-On Agent > Configure Fortinet Single Sign-On Agent**.
2. Enter the following information.

Monitoring user logon events	By default, this is enabled to automatically authenticate users as they log on to the Windows domain. Disable the Monitor feature only if you have a large network where this feature will slow responses too much.
Support NTLM authentication	By default, this is enabled to facilitate logon of users who are connected to a domain that does not have the FSSO DC Agent installed. Disable NTLM authentication only if your network does not support NTLM authentication for security or other reasons.
Collector Agent Status	Shows RUNNING when Collector agent is active.
Listening ports	You can change FSSO Collector Agent related port numbers if necessary.

	FortiGate	TCP port for FortiGate units. Default 8000.
	DC Agent	UDP port for DC Agents. Default 8002.
Logging		
	Log level	Select the minimum severity level of logged messages.
	Log file size limit (MB)	Enter the maximum size for the log file in MB. Default is 10.
	View Log	View all Fortinet Single Sign On agent logs.
	Log logon events in separate logs	Record user login-related information separately from other logs. The information in this log includes: • data received from DC agents • user logon/logoff information • workstation IP change information • data sent to FortiGate units
	View Logon Events	If **Log logon events in separate logs** is enabled, you can view user login-related information.
Authentication		
	Require authenticated connection from FortiGate	Select to require the FortiGate unit to authenticate before connecting to the Collector agent.
	Password	Enter the password that FortiGate units must use to authenticate. The maximum password length is 16 characters. The default password is “fortinetcanada”. It is highly recommended to modify this password.
Timers		
	Workstation verify interval (minutes)	Enter the interval in minutes at which the Fortinet Single Sign On Collector agent connects to client computers to determine whether the user is still logged on. The default is every 5 minutes. The interval may be increased if your network has too much traffic. **Note:** This verification process creates security log entries on the client computer. If ports 139 or 445 cannot be opened on your network, set the interval to 0 to prevent checking. See Configuring FSSO ports on page 148.

	Dead entry timeout interval	Enter the interval in minutes after which Fortinet Single Sign On Agent purges information for user logons that it cannot verify. The default is 480 minutes (8 hours). Dead entries usually occur because the computer is unreachable (such as in standby mode or disconnected) but the user has not logged off. A common reason for this is when users forget to logoff before leaving the office for the day. You can also prevent dead entry checking by setting the interval to 0.
	IP address change verify interval	Fortinet Single Sign On Agent periodically checks the IP addresses of logged-in users and updates the FortiGate unit when user IP addresses change. IP address verification prevents users from being locked out if they change IP addresses, as may happen with DHCP assigned addresses. Enter the verification interval in seconds. The default is 60 seconds. You can enter 0 to prevent IP address checking if you use static IP addresses. This does not apply to users authenticated through NTLM.
Cache user group lookup result		Enable caching. Caching can reduce group lookups and increase performance.
	Cache expire in (minutes)	Fortinet Single Sign On Agent caches group information for logged-in users. Enter the duration in minutes after which the cache entry expires. If you enter 0, the cache never expires. A long cache expire interval may result in more stale user group information. This can be an issue when a user's group information is changed.
	Clear Group Cache	Clear group information of logged-in users. This affects all logged-in users, and may force them to re-logon.

3. You can select **Save&Close** now or leave the agent configuration window open to complete additional configuration in the following sections.

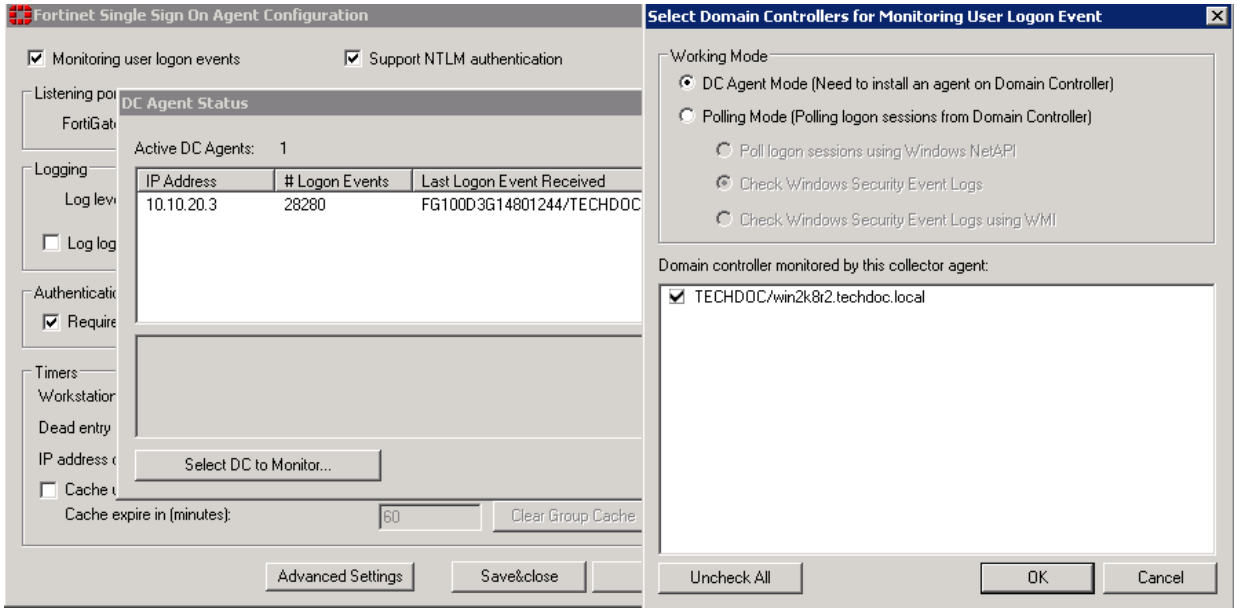
To view the version and build number information for your FSSO Collector Agent configuration, selecting the Fortinet icon in the upper left corner of the Collector agent Configuration screen and select **About Fortinet Single Sign On Agent configuration.**

Selecting Domain Controllers and working mode for monitoring

You can change which DC agents are monitored or change the working mode for logon event monitoring between DC agent mode and polling mode.

When polling mode is selected, it will poll port 445 of the domain controller every few seconds to see who is logged on.

1. From the Start menu select **Programs > Fortinet Fortinet Single Sign-On Agent > Configure Fortinet Single Sign On Agent**.
2. In the **Common Tasks** section, select **Show Monitored DCs**.
3. Select **Select DC to Monitor**.



4. Choose the **Working Mode:**
   - **DC Agent mode** — a Domain Controller agent monitors user logon events and passes the information to the Collector agent. This provides reliable user logon information, however you must install a DC agent on every domain controller in the domain.
   - **Polling mode** — the Collector agent polls each domain controller for user logon information. Under heavy system load this might provide information less reliably. However installing a DC agent on each domain controller is not required in this mode.
5. You also need to choose the method used to retrieve logon information:
   - Poll logon sessions using Windows NetAPI
   - Check Windows Security Event Logs
   - Check Windows Security Event Logs using WMI

   For more information about these options, see Polling mode on page 129.
6. Select **OK**.
7. Select **Close**.
8. Select **Save & Close**.

Configuring Directory Access settings

The FSSO Collector Agent can access Windows Active Directory in one of two modes:

- Standard — the FSSO Collector Agent receives group information from the Collector agent in the **domain\user** format. This option is available on FortiOS 3.0 and later.
- Advanced — the FSSO Collector Agent obtains user group information using LDAP. The benefit of this method is that it is possible to nest groups within groups. This is option is available on FortiOS 3.0 MR6 and later. The group information is in standard LDAP format.

If you change AD access mode, you must reconfigure your group filters to ensure that the group information is in the correct format.

To configure Directory Access settings:

1. From the Start menu select **Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent**.
2. In the **Common Tasks** section, select **Set Directory Access Information**.
   The **Set Directory Access Information** dialog box opens.
3. From the **AD access mode** list, select either **Standard** or **Advanced**.
4. If you selected Advanced AD access mode, select **Advanced Setting** and configure the following settings and then select **OK**:

AD server address	Enter the address of your network's global catalog server.
AD server port	The default AD server port is 3268. This must match your server port.
BaseDN	Enter the Base distinguished name for the global catalog. This is the point in the tree that will be considered the starting point by default-See following example.
Username	If the global catalog accepts your Fortinet Single Sign On Agent agent's credentials, you can leave these fields blank. Otherwise, enter credentials for an account that can access the global catalog.
Password	

BaseDN example

An example DN for Training Fortinet Canada is `ou=training, ou=canada, dc=fortinet, dc=com`. If you set the **BaseDN** to `ou=canada, dc=fortinet, dc=com` then when Fortinet Single Sign On Agent is looking up user credentials, it will only search the Canada organizational unit, instead of all the possible countries in the company. Its a short cut to entering less information and faster searches.

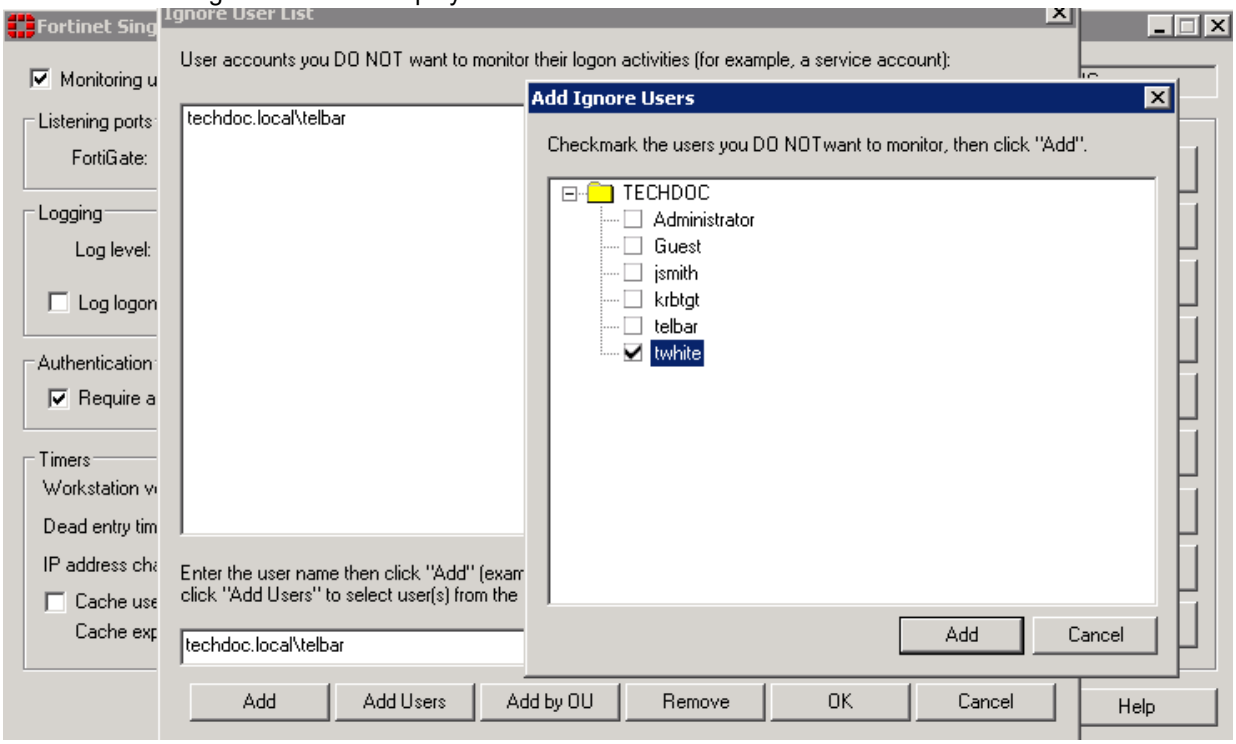
However, you may have problems if you narrow the BaseDN too much when you have international employees from the company visiting different offices. If someone from Fortinet Japan is visiting the Canada office in the example above, their account credentials will not be matched because they are in `ou=japan, dc=fortinet, dc=com` instead of the BaseDN `ou=canada, dc=fortinet, dc=com`. The easy solution is to change the BaseDN to simply be `dc=fortinet, dc=com`. Then any search will check all the users in the company.

Configuring the Ignore User List

The Ignore User List excludes users that do not authenticate to any FortiGate unit, such as system accounts. The logons of these users are not reported to FortiGate units. This reduces the amount of required resources on the FortiGate unit especially when logging logon events to memory.

To configure the Ignore User List:

1. From the Start menu select **Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent**.
2. In the **Common Tasks** section, select **Set Ignore User List**.
   The current list of ignored users is displayed:



3. Do any of the following:
   - To remove a user from the list, select the the username and then select **Remove**. The user's login is no longer ignored.
   - To add users to be ignored,
     - enter the username in the format **domain\username** and select **Add** or
     - select **Add Users**, an **Add Ignore Users** window is displayed, checkmark the users you do not want to monitor, then select **Add** or
     - select **Add by OU**, an **Add Ignore Users by OU** window is displayed, select an OU from the directory tree, then select **Add**. All users under the selected OU will be added to the ignore user list.
4. Select **OK**.

Configuring FortiGate group filters

FortiGate group filters actively control which user logon information is sent to each FortiGate unit. You need to configure the group filter list so that each FortiGate unit receives the correct user logon information for the user groups that are named in its security policies. These group filters help limit the traffic sent to the FortiGate unit, and help limit the logon events logged.

The maximum number of Windows AD user groups allowed on a FortiGate depends on the model. Low end models support 256 Windows AD user groups, where mid and high end models support 1024 groups. This is per VDOM if VDOMs are enabled on the FortiGate unit.

You do not need to configure a group filter on the Collector agent if the FortiGate unit retrieves group information from Windows AD using LDAP. In that case, the Collector agent uses the list of groups you selected on the FortiGate unit as its group filter.

The filter list is initially empty. You need to configure filters for your FortiGate units using the Add function. At a minimum, create a default filter that applies to all FortiGate units without a defined filter.

If no filter is defined for a FortiGate unit and there is no default filter, the Collector agent sends all Windows AD group and user logon events to the FortiGate unit. While this normally is not a problem, limiting the amount of data sent to the FortiGate unit improves performance by reducing the amount of memory the unit uses to store the group list and resulting logs.

To configure a FortiGate group filter:

1. From the Start menu select **Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent**.
2. In the **Common Tasks** section, select **Set Group Filters**.
   The FortiGate Filter List opens. It has the following columns:

FortiGate SN	The serial number of the FortiGate unit to which this filter applies.
Description	An optional description of the role of this FortiGate unit.
Monitored Groups	The Windows AD user groups that are relevant to the security policies on this FortiGate unit.
Add	Create a new filter.
Edit	Modify the filter selected in the list.
Remove	Remove the filter selected in the list.
OK	Save the filter list and exit.
Cancel	Cancel changes and exit.

3. Select **Add** to create a new filter. If you want to modify an existing filter, select it in the list and then select **Edit**.
4. Enter the following information and then select **OK**.

Default filter	Select to create the default filter. The default filter applies to any FortiGate unit that does not have a specific filter defined in the list.
FortiGate Serial Number	Enter the serial number of the FortiGate unit to which this filter applies. This field is not available if Default is selected.
Description	Enter a description of this FortiGate unit's role in your network. For example, you could list the resources accessed through this unit. This field is not available if Default is selected.
Monitor the following groups	The Collector agent sends to the FortiGate unit the user logon information for the Windows AD user groups in this list. Edit this list using the Add, Advanced and Remove buttons.
Add	In the preceding single-line field, enter the Windows AD domain name and user group name, and then select Add. If you don't know the exact name, use the Advanced button instead. The format of the entry depends on the AD access mode (see Configuring Directory Access settings on page 145): Standard: Domain\Group Advanced: cn=group, ou=corp, dc=domain
Advanced	Select **Advanced**, select the user groups from the list, and then select **Add**.
Remove	Remove the user groups selected in the monitor list.

Configuring FSSO ports

For FSSO to function properly a small number of TCP and UDP ports must be open through all firewalls on the network. There ports listed in this section assume the default FSSO ports are used.

TCP ports for FSSO agent with client computers

Windows AD records when users log on but not when they log off. For best performance, Fortinet Single Sign On Agent monitors when users log off. To do this, Fortinet Single Sign On Agent needs read-only access to each client computer's registry over TCP port 139 or 445. Open at least one of these ports — ensure it is not blocked by firewalls.

If it is not feasible or acceptable to open TCP port 139 or 445, you can turn off Fortinet Single Sign On Agent logoff detection. To do this, set the Collector agent **workstation verify interval** to 0. The FSSO Collector Agent assumes that the logged on computer remains logged on for the duration of the Collector agent dead entry timeout interval — by default this is eight hours.

Configuring ports on the Collector agent computer

On the computer where you install the Collector agent, you must make sure that the firewall does not block the listening ports for the FortiGate unit and the DC Agent. By default, these are TCP port 8000 and UDP port 8002.

For more information about setting these ports, see Configuring FSSO Advanced Settings on page 155.

Configuring alternate user IP address tracking

In environments where user IP addresses change frequently, you can configure Fortinet Single Sign On Agent to use an alternate method to track user IP address changes. Using this method, Fortinet Single Sign On Agent responds more quickly to user IP address changes because it directly queries workstation IP addresses to match users and IP addresses.

This feature requires FSAE version 3.5.27 or later, Fortinet Single Sign On Agent any version, and FortiOS 3.0 MR7 or later.

To configure alternate user IP address tracking:

1. On the computer where the Collector agent is installed, go to **Start > Run**.
2. Enter `regedit` or `regedt32` and select **OK**.
   The Registry Editor opens.
3. Find the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FSAE\collectoragent.
4. Set the supportFSAEauth value (dword) to 00000001.
   If needed, create this new dword.
5. Close the Registry Editor.
6. From the Start menu select **Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent**.
7. Select **Apply**.
   The Fortinet Single Sign On Agent service restarts with the updated registry settings.

Viewing FSSO component status

It is important to know the status of both your Collector agents and DC agents.

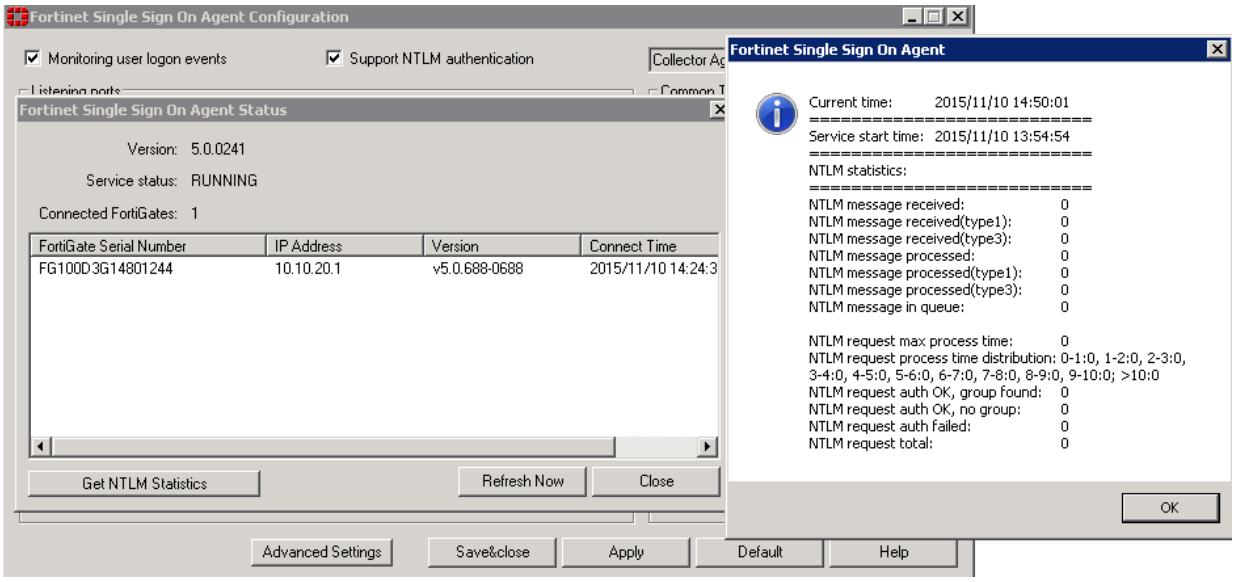
Viewing Collector agent status

Use the **Show Service Status** to view your Collector agent information in the Status window. The Status window displays:

- the version of the software
- the status of the service
- the number of connected FortiGate units
- connected FortiGate information such as serial number, IP address, and connect time

To view Collector agent status:

1. From the Start menu select **Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent**.
2. In the **Common Tasks** section, select **Show Service Status**.
   The Fortinet Single Sign On Collector agent Status window opens.
3. Optionally select **Get NTLM statistics** in the Status window to display NTLM information such as number of messages received, processed, failed, in the queue.



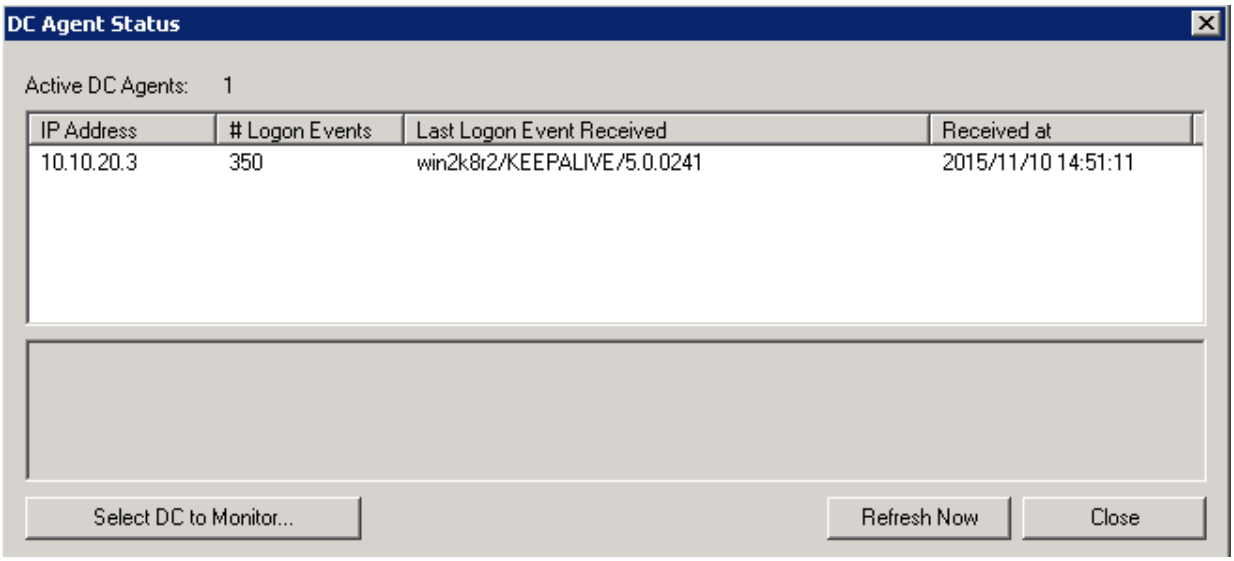
Viewing DC agent status

Use the **Show Monitored DCs** to view the status of DC agents.

To view domain controller agent status:

1. From the Start menu select **Programs > Fortinet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent**.
2. In the **Common Tasks** section, select **Show Monitored DCs**.
   For each DC Agent, the following information is displayed:
   - IP address
   - number of logon events received
   - the last logon event
   - when last logon was received

To change which DC agents are monitored or change the working mode for logon event monitoring, select **Select DC to Monitor**



Configuring the FSSO TS agent for Citrix

The FSSO TS agent works with the same FSSO Collector agent that is used for integration with Windows Active Directory. Install the Collector agent first. Follow the Collector agent installation procedure in Collector agent installation on page 135.

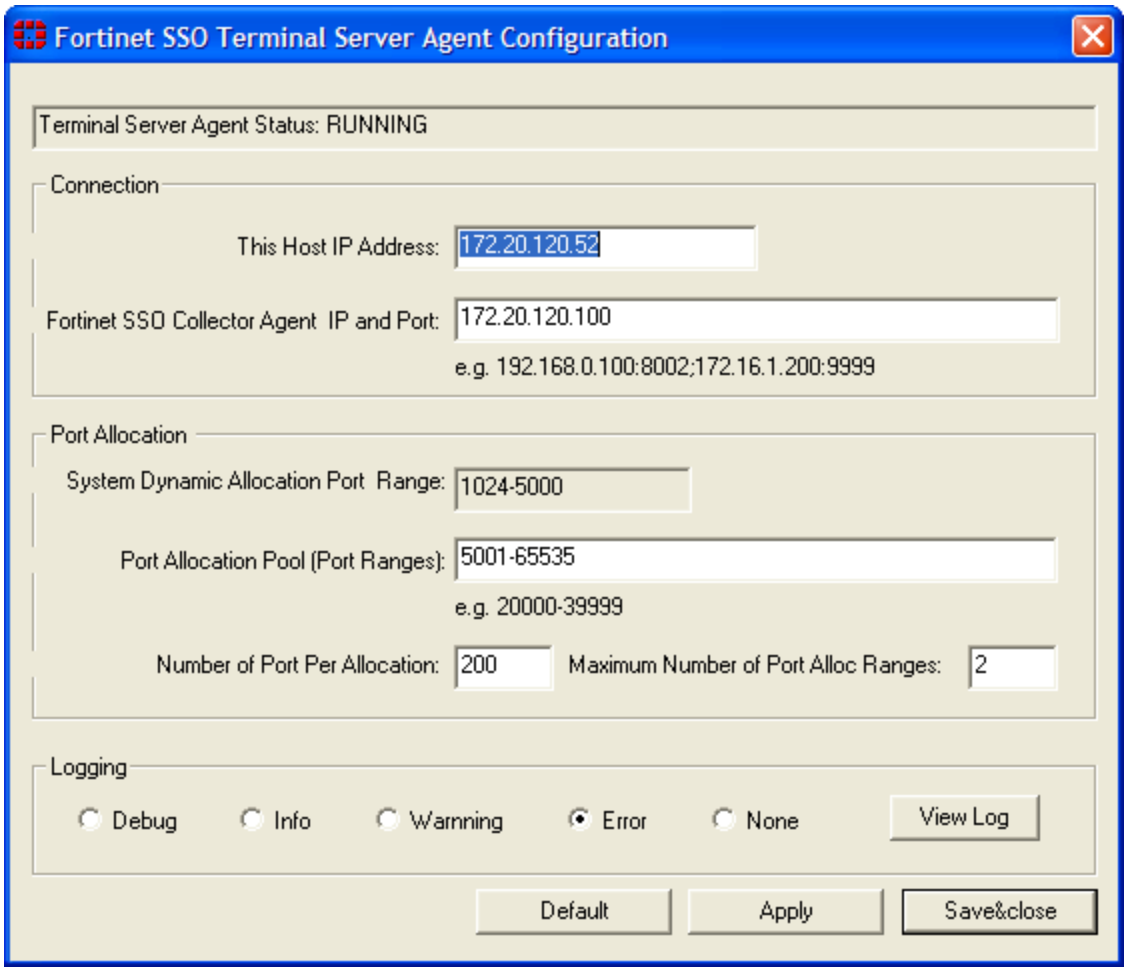
Configuration steps include:

- Install the Fortinet Citrix FSSO agent on the Citrix server.
- Install the Fortinet FSSO collector on a server on the network.
- Add the Citrix FSSO agent to the FortiGate Single-sign-On configuration.
- Add Citrix FSSO groups and users to an FSSO user group.
- Add an FSSO identity-based security policy that includes the Citrix FSSO user groups.

To change the TS agent configuration, select from the Start menu **Programs > Fortinet > Fortinet Single Sign-On Agent > TSAgent Config**. In addition to the host and Collector agent IP addresses that you set during installation, you can adjust port allocations for Citrix users. When a Citrix user logs on, the TS agent assigns that user a range of ports. By default each user has a range of 200 ports.

Fortinet SSO Collector Agent IP and Port needs to point to the current configured listening port on the collector which is port 8002 by default. Though it may be configured to a custom port.

Configuring the TS agent



Configuring FSSO with Novell networks

You need to configure the eDirectory agent for it to communicate with eDirectory servers. You may have provided some of this information during installation.

This section includes:

- Configuring the eDirectory agent
- Adding an eDirectory server
- Configuring a group filter

Configuring the eDirectory agent

You need to configure the eDirectory agent for it to communicate with eDirectory servers.

To configure the eDirectory agent:

1. From the Start menu select **Programs > Fortinet > eDirectory Agent > eDirectory Config Utility**.
2. The eDirectory Agent Configuration Utility dialog opens. Enter the following information and select **OK**.

eDirectory Authentication	
Username	Enter a username that has access to the eDirectory, using LDAP format.
Password	Enter the password.
Listening port	Enter the TCP port on which Fortinet Single Sign On Agent listens for connections from FortiGate units. The default is 8000. You can change the port if necessary.
Refresh interval	Enter the interval in seconds between polls of the eDirectory server to check for new logons. The default is 30 seconds.

FortiGate Connection Authentication	
Require authenticated connection from FortiGate	Select to require the FortiGate unit to authenticate before connecting to the eDirectory Agent.
Password	Enter the password that FortiGate units must use to authenticate. The maximum password length is 16 characters. The default password is “FortinetCanada”.
User logon Info Search Method	Select how the eDirectory agent accesses user logon information: **LDAP** or **Native** (Novell API). LDAP is the default. If you select **Native**, you must also have the Novell Client installed on the PC.

Logging	
Log file size limit (MB)	Enter the maximum size for the log file in MB.
View Log	View the current log file.
Dump Session	List the currently logged-on users in the log file. This can be useful for troubleshooting.
Log level	Select **Debug, Info**, **Warning** or **Error** as the minimum severity level of message to log or select **None** to disable logging.

eDirectory Server List	
Add	Add an eDirectory server. See Adding an eDirectory server on page 154.
Delete	Delete the selected eDirectory server.

eDirectory Server List	
Edit	Modify the settings for the selected server.
Set Group Filters...	Select the user groups whose user logons will be reported to the FortiGate unit. This is used only if user groups are not selected on the FortiGate unit.

Adding an eDirectory server

Once the eDirectory agent is configured, you add one or more eDirectory servers.

To add an eDirectory server:

1. In the eDirectory Agent Configuration Utility dialog box (see the preceding procedure, Configuring the eDirectory agent), select **Add**.
2. The eDirectory Setup dialog box opens. Enter the following information and select OK:

eDirectory Server Address	Enter the IP address of the eDirectory server.
Port	If the eDirectory server does not use the default port 389, clear the **Default** check box and enter the port number.
Use default credential	Select to use the credentials specified in the eDirectory Configuration Utility. See Configuring the eDirectory agent on page 152. Otherwise, leave the check box clear and enter a username and Password below.
User name	Enter a username that has access to the eDirectory, using LDAP format.
User password	Enter the password.
Use secure connection (SSL)	Select to connect to the eDirectory server using SSL security.
Search Base DN	Enter the base Distinguished Name for the user search.

Configuring a group filter

The eDirectory agent sends user logon information to the FortiGate unit for all user groups unless you either configure an LDAP server entry for the eDirectory on the FortiGate unit and select the groups that you want to monitor or configure the group filter on the eDirectory agent.

If both the FortiGate LDAP configuration and the eDirectory agent group filter are present, the FortiGate user group selections are used.

To configure the group filter:

1. From the Start menu select **Programs > Fortinet > eDirectory Agent > eDirectory Config Utility**.
2. Select **Set Group Filters**.
3. Do one of the following:
   - Enter group names, then select **Add**.
   - Select **Advanced**, select groups, and then select **Add**.

4. Select **OK**.

Configuring FSSO Advanced Settings

Depending on your network topologies and requirement, you may need to configure advanced settings in the FSSO Colloctor agent.To do so, from the Start menu, select **Programs > Fortinet > Fortinet Single Sign-On Agent > Configure Fortinet Single Sign-On Agent**, then from the **Common Tasks** section, select **Advanced Settings**.

This section include :

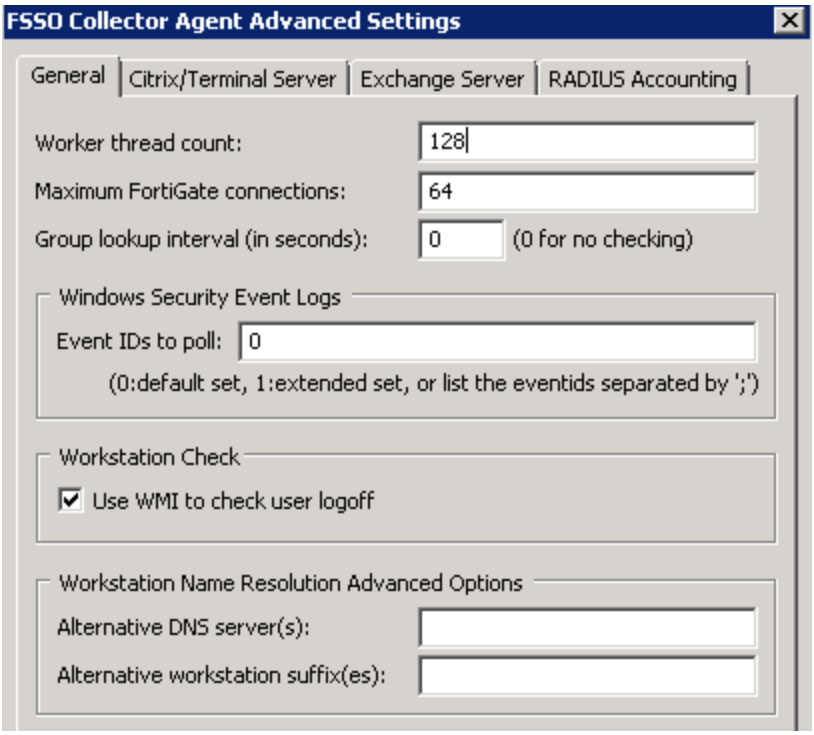
- General Settings
- Citrix/Terminal Server
- Exchange Server
- RADIUS Accounting

General Settings

In the General tab, enter the following information and select **OK**.

Worker thread count	Number of threads started in the CA process. Default is128 on CA version 5.0.0241.
Maximum FortiGate connections	Number of FortiGates can be connected to the CA. Default is 64.
Group look-up interval	The interval in seconds to lookup users/groups. If an AD group membership of currently logged on user, CA can detect this and update information on the FortiGate. Enter 0 for no checking.
Windows security Event logs	Choose the event logs to poll.
Event IDs to poll	0:Default set, it includes Kerberos authentication event logs : 672 for Windows server 2003, 4768 for Windows server 2008 and 2012 and NTLM authentication event logs : 680 for Windows server 2003, 4776 for Windows server 2008 and 2012. 1: Extended set, it includes Kerberos service ticket event logs : 673 for Windows server 2003, 4769 for Windows server 2008 and 2012. Service tickets are obtained whenever a user or computer accesses a server on the network. List the event ids separated by ";".
Workstation Check	Optianally enable **Use WMI to check user logoff** for the collector agent to query whether users is still logged on.
Workstation Name Resolution Advance Options	

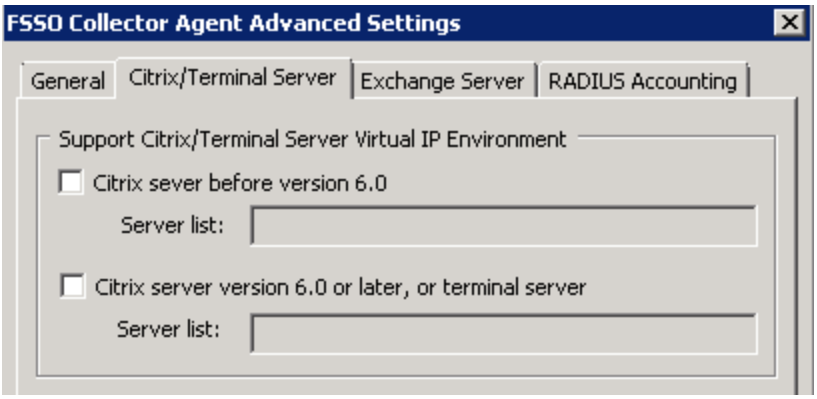
Alternative DNS server(s)	Collector Agent uses the DNS server configured on the machine it is running on by default. If CA should use another DNS server then one or more alternative DNS server can be configured here.
Alternative workstation suffix(es)	If only host name is available CA uses the default domain suffix to build a FQDN for DNS queries. In case CA should use a different suffix, it can be configured as well.



Citrix/Terminal Server

In the Citrix/Terminal Server tab, enter the following information and select **OK**.

Support Citrix/Terminal Server Virtual IP Environment	When Citrix server are configured with VIP, CA can get user logon events from theses server. Citrix changed their interface and data format so version of Citrix server is important.
Citrix server before version 6.0	Enable this option if you Citrix server version is before 6.0.
Server list	Enter the list of servers separated by colon.
Citrix server version 6.0 or later, or Terminal Server	Enable this option if you Citrix server version is 6.0 or later.
Server list	Enter the list of servers separated by colon.

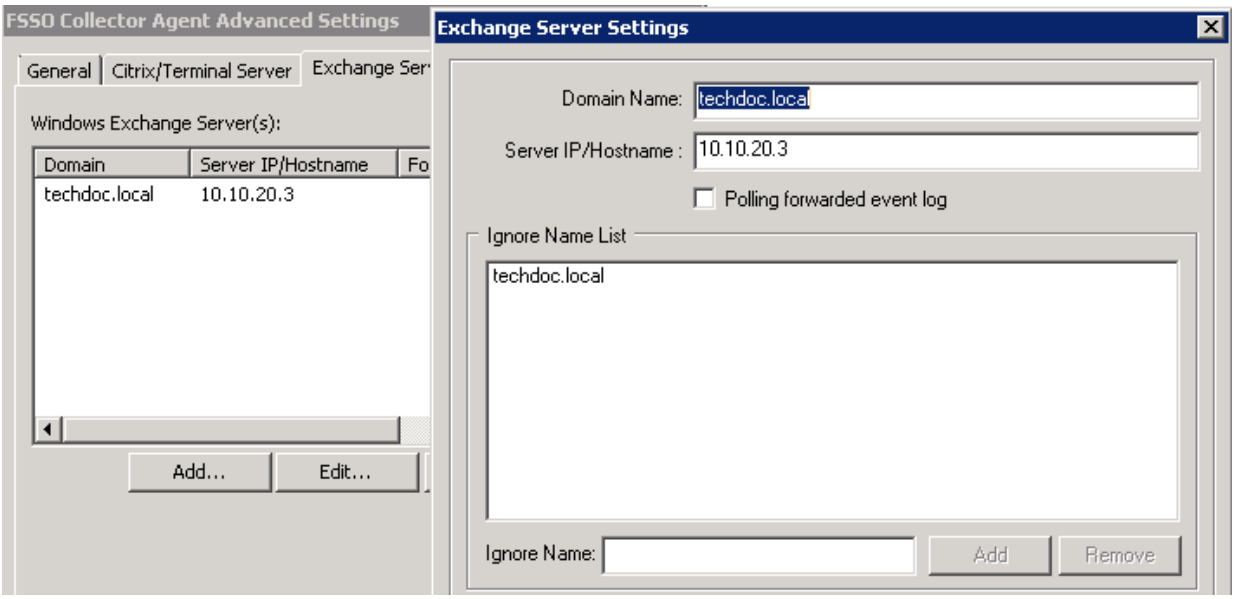


Exchange Server

FSSO supports monitoring Microsoft Exchange Server. This is useful for situation that the user use the domain account to access their email, but client device might or might not be in the domain. Support for Exchange server is configured on the Back-end FSSO collector agent under **Advanced Settings** > **Exchange Server**.

Select **Add** and enter the following information and select **OK**.

Domain Name	Enter your domain name.
Server IP/Hostname	Enter the IP address or the hostname of your exchange server.
Polling forwarded event log	This option for scenarios when you do not want that CA polls the Exchange Server logs directly. In this case you need to configure event log forwarding on the Exchange server. Exchange event logs can be forwarded to any member server. If you enable this, instead of the IP of the Exchange server configured in the previous step, you must then configure the IP of this member server. CA will then contact the member server.
Ignore Name	Because CA will also check Windows log files for logon events and when a user authenticates to Exchange Server there is also a logon event in Windows event log, which CA will read and this will overwrite the Exchange Server logon event (ES-EventLog) on CA. So it is recommended to set the ignore list to the domain the user belongs to. To do so, enter the domain name in the **Ignore Name** field and select **Add**.



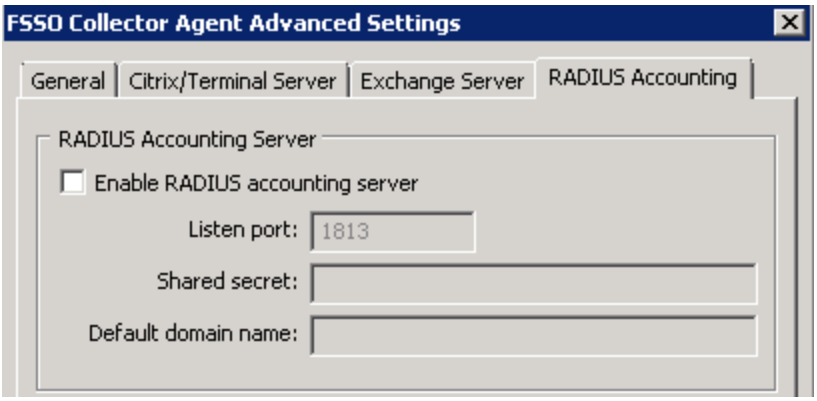
RADIUS Accounting

A RADIUS server must be configured in your network to send accounting messages to the Collector Agent which can be configured to work with most RADIUS-based accounting systems. In most cases, you only need to do the following to your RADIUS accounting system:

- Add a user group name field to customer accounts on the RADIUS server so that the name is added to the RADIUS Start record sent by the accounting system to the Collector Agent. User group names do not need to be added for all users, only to the accounts of users who will use RADIUS Accounting feature on the Collector Agent.
- Configure your accounting system to send RADIUS Start records to the Collector Agent.

The Collocter Agent should be configured to listen for RADIUS accounting messages as following.

RADIUS Accounting Server	
Enable RADIUS Accounting Server	Enable this option to allow the CA to gather information about authenticated users via a RADIUS server and send these information to the FortiGate unit for monitoring.
Listen port	The port on which CA listens for RADIUS accounting messages. Default RADIUS accounting is 1813, but if RADIUS server sends accounting messages on different port, value can be configured here.
Shared secret	Common secret between CA and RADIUS server.
Default domain name	This should be the AD domain for which this CA is configured. In this case user name in RADIUS accounting message can be in simple format like `user1`. If this value is empty, then user name in RADIUS accounting message must be in one of these formats `user1@domain`, `Domain\user1` or `domain/user1`. CA will use user name and domain to query group membership of user. Client IP address (Framed IP) should also be in RADIUS accounting message, so that CA can forward user name, IP address and groups to the FortiGate.



Configuring FSSO on FortiGate units

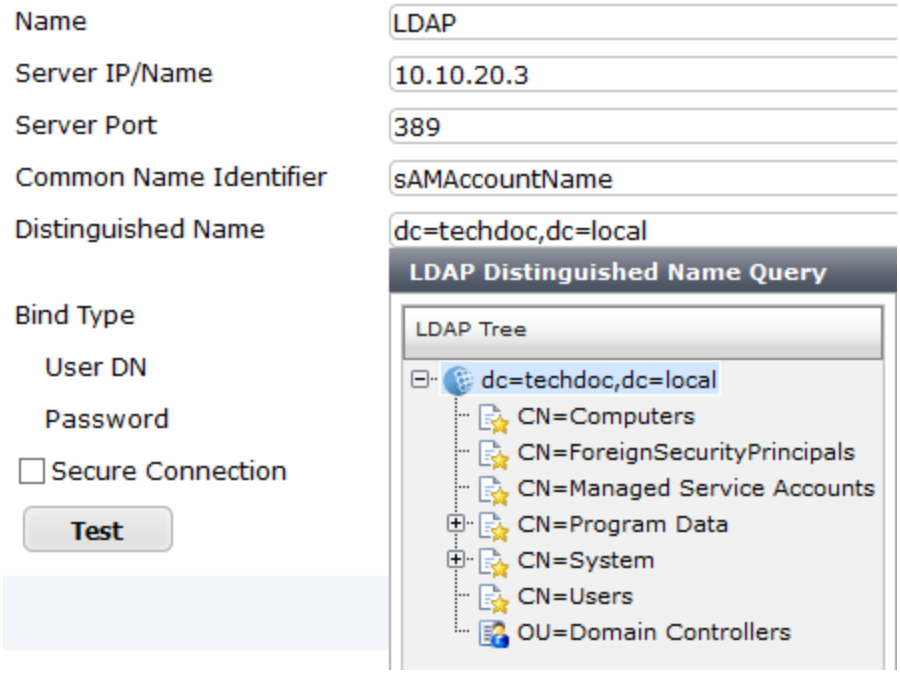
To configure your FortiGate unit to operate with agent-based FSSO, you

- Configure any access to LDAP servers that might be necessary. Skip this step if you are using FSSO Standard mode. See Configuring LDAP server access on page 159.
- Specify the Collector agent or Novell eDirectory agent that will provide user logon information. See Specifying your Collector agents or Novell eDirectory agents on page 161.
- Add Active Directory user groups to FortiGate user groups. See Creating Fortinet Single Sign-On (FSSO) user groups on page 162.
- Create security policies for FSSO-authenticated groups. See Creating security policies on page 163.
- Optionally, specify a guest security policy to allow guest access. See Enabling guest access through FSSO security policies on page 164.

Configuring LDAP server access

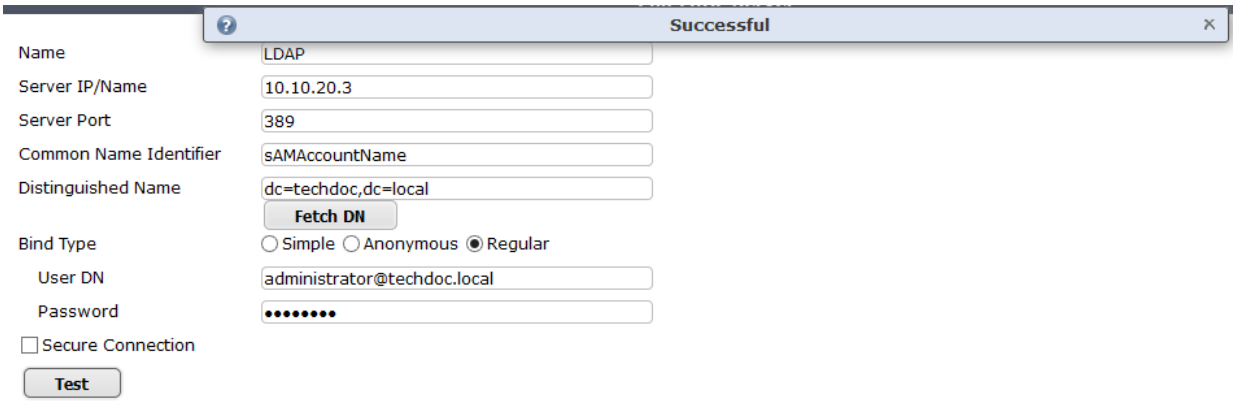
LDAP access is required if your network has a Novell eDirectory agent or a Collector agent using Windows Advanced AD access mode. If you are using FSSO Standard mode, go to Specifying your Collector agents or Novell eDirectory agents on page 161.

1. Go to **User & Device > Authentication > LDAP Servers** and select **Create New**.
2. Enter the **Server IP/Name** and **Server Port** (default 389).
3. In the **Common Name Identifier** field, enter **sAMAccountName**.The default common name identifier is `cn`. This is correct for most LDAP servers. However some servers use other identifiers such as `uid`.
4. In the **Distinguished Name** field, enter your organization distinguished name. In this example, Distinguished Name is dc=techdoc,dc=local
5. Select **Fetch DN**, this will fetch the Windows AD directory.



6. Set **Bind Type** to **Regular.**
7. In the **User DN** field, enter the administrative account name that you created for FSSO.
   For example, if the account is administrator, enter “administrator@techdoc.local”.
8. Enter the administrative account password in the **Password** field.
9. Optionally select **Secure Connection**.
   - In the **Protocol** field, select **LDAPS** or **STARTTLS**.
   - In the **Certificate** field, select the appropriate certificate for authentication.

   Note that you need to configure the Windows AD for secure connection accordingly.
10. Select **OK**.
11. Test your configuration by selecting the **Test** button. A successful message confirming the right settings appears.



To configure LDAP for FSSO - CLI example:

```
config user ldap
   edit LDAP
      set server 10.10.20.3
```

```
        set cnid sAMAccountName
        set dn dc=techdoc,dc=local
        set type regular
        set username administrator@techdoc.local
        set password <your_password>
    next
end
```

Specifying your Collector agents or Novell eDirectory agents

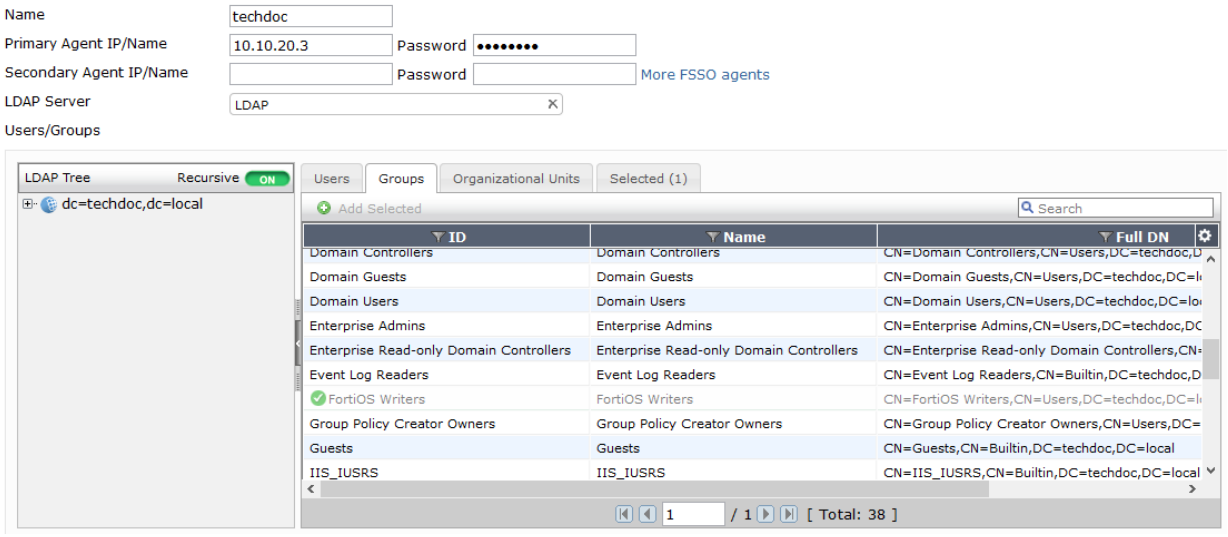
You need to configure the FortiGate unit to access at least one Collector agent or Novell eDirectory agent. You can specify up to five servers on which you have installed a Collector or eDirectory agent. The FortiGate unit accesses these servers in the order that they appear in the list. If a server becomes unavailable, the next one in the list is tried.

To specify Collector agents - web-based manager:

1. Go to **User & Device > Authentication > Single Sign-On** and select **Create New**.
2. In **Type**, select **Fortinet Single-Sign-On Agent**.
3. Enter a **Name** for the Windows AD server. This name appears in the list of Windows AD servers when you create user groups.
4. Enter the following information for each of up to five collector agents and select **OK**:

Agent IP/Name	Enter the IP address or the name of the server where this agent is installed. Maximum name length is 63 characters. If the TCP port used for FSSO is not the default, 8000, you can change the setting in the CLI using the `config user fsso` command. See Configuring Collector agent settings on page 141.
Password	Enter the password for the Collector agent or eDirectory agent. For the Collector agent, this is required only if you configured the agent to require authenticated access.

5. For Novell eDirectory or Windows AD with Collector agent in Advanced AD access mode select the **LDAP Server** you configured previously. See Configuring LDAP server access on page 159.
6. In **Users/Groups**, select the **Users** or **Groups** or **Organizational Units** tab and then select the users or groups or OU that you want to monitor.
7. Select **OK**.



To specify the FSSO Collector agent - CLI:

In this example, the SSO server name is techdoc and the LDAP server is LDAP.

```
config user fsso
   edit techdoc
      set ldap-server LDAP
      set password <your_password>
      set server 10.10.20.3
      set port 8000
   end
```

Creating Fortinet Single Sign-On (FSSO) user groups

You cannot use Windows or Novell groups directly in FortiGate security policies. You must create FortiGate user groups of the FSSO type and add Windows or Novell groups to them.

To create a user group for FSSO authentication - web-based manager:

1. Go to **User & Device > User > User Groups**.
2. Select **Create New**.
   The New User Group dialog box opens.
3. In the **Name** box, enter a name for the group, FSSO_Internet_users for example.
4. In **Type**, select **Fortinet Single Sign-On (FSSO)**.
5. In **Members**, select the required **FSSO** groups.
6. Select **OK**.

To create the FSSO_Internet-users user group - CLI :

```
config user group
   edit FSSO_Internet_users
      set group-type fsso-service
      set member CN=Engineering,cn=users,dc=office,dc=example,dc=com
          CN=Sales,cn=users,dc=office,dc=example,dc=com
   end
```

Creating security policies

Policies that require FSSO authentication are very similar to other security policies. Using identity-based policies, you can configure access that depends on the FSSO user group. This allows each FSSO user group to have its own level of access to its own group of services

In this situation, Example.com is a company that has its employees and authentication servers on an internal network. The FortiGate unit intercepts all traffic leaving the internal network and requires FSSO authentication to access network resources on the Internet. The following procedure configures the security policy for FSSO authentication. FSSO is installed and configured including the RADIUS server, FSSO Collector agent, and user groups on the FortiGate

For the following procedure, the internal interface is `port1` and the external interface connected to the Internet is `port2`. There is an address group for the internal network called `company_network`. The FSSO user group is called `fsso_group`, and the FSSO RADIUS server is `fsso_rad_server`.

To configure an FSSO authentication security policy - web-based manager:

1. Go to **Policy & Objects > Policy > IP4** and select **Create New**.
2. Enter the following information.

Incoming Interface	port1
Source Address	company_network
Source User(s)	`fsso_group`
Outgoing Interface	port2
Destination Address	all
Schedule	always
Service	HTTP, HTTPS, FTP, and Telnet
Action	ACCEPT
NAT	ON
UTM Security Profiles	ON for AntiVirus, IPS, Web Filter, and Email Filter, all using default profiles.
Log Allowed Traffic	ON. Select **Security Events**.

3. Select **OK**.
4. Ensure the FSSO authentication policy is higher in the policy list than more general policies for the same interfaces.

To create a security policy for FSSO authentication - CLI:

```
config firewall policy
   edit 0
      set srcintf port1
      set dstintf port2
```

```
    set srcaddr company_network
    set dstaddr all
    set action accept
    set groups fsso_group
    set schedule always
    set service HTTP HTTPS FTP TELNET
    set nat enable
end
```

Here is an example of how this FSSO authentication policy is used. Example.com employee on the internal company network logs on to the internal network using their RADIUS username and password. When that user attempts to access the Internet, which requires FSSO authentication, the FortiGate authentication security policy intercepts the session, checks with the FSSO Collector agent to verify the user's identity and credentials, and then if everything is verified the user is allowed access to the Internet.

Users belonging to multiple groups

Before FSSO 4.0 MR3, if a user belonged to multiple user groups, the first security policy to match any group that user belonged too was the only security policy applied. If that specific group did not have access to this protocol or resource where another group did, the user was still denied access. For example, `test_user` belongs to `group1` and `group2`. There are two FSSO authentication policies — one matches `group1` to authenticate FTP traffic and one matches `group2` to authenticate email traffic. The `group1` policy is at the top of the list of policies. If `test_user` wants to access an email server, the first policy encountered for a group `test_user` belongs to is the `group1` policy which does not allow email access and `test_user` is denied access. This is despite the next policy allowing access to email. If the order was reversed in this case, the traffic would be matched and the user's traffic would be allowed through the firewall. However if the policy order was reversed, FTP traffic would not be matched.

As of FSSO 4.0 MR3, if a user belongs to multiple groups multiple then attempts to match the group are attempted if applicable. Using the above example, when the attempt to match the `group1` policy is made and fails, the next policy with a group that `test_user` is a member of is attempted. In this case, the next policy is matched and access is granted to the email server.

When configuring this example the only difference between the policies is the services that are listed and the FSSO user group name.

Authenticating through multiple groups allows administrators to assign groups for specific services, and users who are members of each group have access to those services. For example there could be an FTP group, an email group, and a Telnet group.

Enabling guest access through FSSO security policies

You can enable guest users to access FSSO security policies. Guests are users who are unknown to the Windows AD or Novell network and servers that do not logon to a Windows AD domain.

To enable guest access in your FSSO security policy, add an identity-based policy assigned to the built-in user group `SSO_Guest_Users`. Specify the services, schedule and protection profile that apply to guest users — typically guests receive reduced access to a reduced set of services. Creating security policies on page 163

FortiOS FSSO log messages

There are two types of FortiOS log messages — firewall and event. FSSO-related log messages are generated from authentication events. These include user logon and log off events, and NTLM authentication events. These log messages are central to network accounting policies, and can also be useful in troubleshooting issues. For more information on firewall logging, see "Enabling security logging". For more information on logging, see the FortiOS Handbook Log and Reporting guide.

Enabling authentication event logging

For the FortiGate unit to log events, that specific type of event must be enabled under logging.

When VDOMs are enabled certain options may not be available, such as CPU and memory usage events. You can enable event logs only when you are logged on to a VDOM; you cannot enable event logs globally.

To ensure you log all the events need, set the minimum log level to Notification or Information. Firewall logging requires Notification as a minimum. The closer to Debug level, the more information will be logged. While this extra information is useful, you must

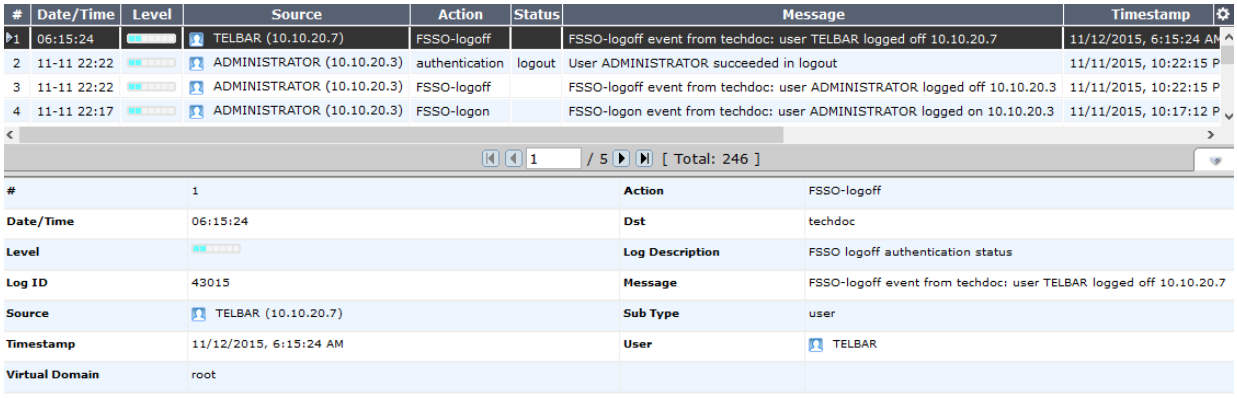
To enable event logging:

1. Go to **Log&Report > Log Config > Log Settings**.
2. In **Event Logging**, select:

System activity event	All system-related events, such as ping server failure and gateway status.
User activity event	All administration events, such as user logins, resets, and configuration updates.

3. Optionally you can enable any or all of the other logging event options.
4. Select **Apply**.

Authentication log messages



#	Date/Time	Level	Source	Action	Status	Message	Timestamp
1	06:15:24		TELBAR (10.10.20.7)	FSSO-logoff		FSSO-logoff event from techdoc: user TELBAR logged off 10.10.20.7	11/12/2015, 6:15:24 AM
2	11-11 22:22		ADMINISTRATOR (10.10.20.3)	authentication	logout	User ADMINISTRATOR succeeded in logout	11/11/2015, 10:22:15 P
3	11-11 22:22		ADMINISTRATOR (10.10.20.3)	FSSO-logoff		FSSO-logoff event from techdoc: user ADMINISTRATOR logged off 10.10.20.3	11/11/2015, 10:22:15 P
4	11-11 22:17		ADMINISTRATOR (10.10.20.3)	FSSO-logon		FSSO-logon event from techdoc: user ADMINISTRATOR logged on 10.10.20.3	11/11/2015, 10:17:12 P

1 / 5 [Total: 246]

#	1	Action	FSSO-logoff
Date/Time	06:15:24	Dst	techdoc
Level		Log Description	FSSO logoff authentication status
Log ID	43015	Message	FSSO-logoff event from techdoc: user TELBAR logged off 10.10.20.7
Source	TELBAR (10.10.20.7)	Sub Type	user
Timestamp	11/12/2015, 6:15:24 AM	User	TELBAR
Virtual Domain	root		

List of FSSO related log messages

Message ID	Severity	Description
43008	Notification	Authentication was successful
43009	Notification	Authentication session failed
43010	Warning	Authentication locked out
43011	Notification	Authentication timed out
43012	Notification	FSSO authentication was successful
43013	Notification	FSSO authentication failed
43014	Notification	FSSO user logged on
43015	Notification	FSSO user logged off
43016	Notification	NTLM authentication was successful
43017	Notification	NTLM authentication failed

For more information on logging, see the FortiOS Handbook Log and Reporting guide.

Testing FSSO

Once FSSO is configured, you can easily test to ensure your configuration is working as expected. For additional FSSO testing, see Troubleshooting FSSO on page 167.

1. Logon to one of the stations on the FSSO domain, and access an Internet resource.
2. Connect to the CLI of the FortiGate unit, and if possible log the output.
3. Enter the following command:
   ```
   diagnose debug authd fsso list
   ```
4. Check the output. If FSSO is functioning properly you will see something similar to the following:
   ```
   ----FSSO logons----
   IP: 10.10.20.3 User: ADMINISTRATOR Groups: CN=FORTIOS WRITERS,CN=USERS,DC=TECHDOC,DC=LOCAL
       Workstation: WIN2K8R2.TECHDOC.LOCAL MemberOf: FortiOS_Writers
   IP: 10.10.20.7 User: TELBAR Groups: CN=FORTIOS WRITERS,CN=USERS,DC=TECHDOC,DC=LOCAL
       Workstation: TELBAR-PC7.TECHDOC.LOCAL
   Total number of logons listed: 2, filtered: 0
   ----end of FSSO logons----
   ```
   The exact information will vary based on your installation.
5. Check the FortiGate event log, for FSSO-auth action or other FSSO related events with FSSO information in the message field.
6. To check server connectivity, run the following commands from the CLI:

```
FGT# diagnose debug enable
FGT# diagnose debug authd fsso server-status
FGT# Server Name Connection Status Version
     ----------- ---------------- -------
     techdoc       connected FSSO 5.0.0241
```

Troubleshooting FSSO

When installing, configuring, and working with FSSO some problems are quite common. A selection of these problems follows including explanations and solutions.

Some common Windows AD problems include:

- General troubleshooting tips for FSSO
- Users on a particular computer (IP address) cannot access the network
- Guest users do not have access to network
- Agent-based FSSO
- User logon events not received by FSSO Collector agent
- Mac OS X users can't access external resources after waking from sleep mode

General troubleshooting tips for FSSO

The following tips are useful in many FSSO troubleshooting situations.

- Ensure all firewalls are allowing the FSSO required ports through.
  FSSO has a number of required ports that must be allowed through all firewalls or connections will fail. These include: ports 139, 389 (LDAP), 445, 636 (LDAP) 8000, and 8002.
- Ensure the Collector agent has at least 64kbps bandwidth to the FortiGate unit.
  If not the Collector agent does not have this amount of bandwidth, information FSSO information may not reach the FortiGate unit resulting in outages. The best solution is to configure traffic shaping between the FortiGate unit and the Collector agent to ensure that minimum bandwidth is always available.

Users on a particular computer (IP address) cannot access the network

Windows AD Domain Controller agent gets the username and workstation where the logon attempt is coming from. If there are two computers with the same IP address and the same user trying to logon, it is possible for the authentication system to become confused and believe that the user on computer_1 is actually trying to access computer_2.

Windows AD does not track when a user logs out. It is possible that a user logs out on one computer, and immediate logs onto a second computer while the system still believes the user is logged on the original computer. While this is allowed, information that is intended for the session on one computer may mistakenly end up going to the other computer instead. The result would look similar to a hijacked session.

Solutions

- Ensure each computer has separate IP addresses.
- Encourage users to logout on one machine before logging onto another machine.

- If multiple users have the same username, change the usernames to be unique.
- Shorten timeout timer to flush inactive sessions after a shorter time.

Guest users do not have access to network

A group of guest users was created, but they don't have access.

Solution

The group of the guest users was not included in a policy, so they do not fall under the guest account. To give them access, associate their group with a security policy.

Additionally, there is a default group called **`SSO_Guest_Users`**. Ensure that group is part of an identity-based security policy to allow traffic.

Can't find the DCagent service

The DCagent service can't be found in the list of regular windows services. This is because it has no associated Windows service.

Instead DCagent is really `dcagent.dll` and is located in the `Windows\system32` folder. This DLL file is loaded when windows boots up and it intercepts all logon events processed by the domain controller to send these events to the Collector agent (CA).

Solution

To verify that the DCagent is installed properly

1. Check that DCagent.dll exists in `Windows\system32` folder.
2. Check that the registry key exists: `[HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FSAE\dcagent]`

If both exist, the DCagent is properly installed.

User logon events not received by FSSO Collector agent

When a warning dialog is present on the screen on the Collector agent computer, the Collector agent will not receive any logon events. Once the dialog has been closed normal operation will resume.

If polling mode is enabled, it is possible the polling interval is too large. Use a shorter polling interval to ensure the collector agent is capturing all logon events.

If NetAPI polling mode is enabled, consider switching to Event logs or Event Logs using WMI polling as it provides better accuracy.

Mac OS X users can't access external resources after waking from sleep mode

When client computers running Mac OS X (10.6.X and higher) wake up from sleep mode, the user must authenticate again to be able to access external resources. If the user does not re-authenticate, the user will maintain access to internal web sites, but will be unable to access any external resources.

This issue is caused by Mac OS X not providing sufficient information to the FSSO. This results in the FortiGate blocking access to the user because they cannot be authenticated.

Solution

The security settings on client computer(s) must be configured to require that a username and password be entered when exiting sleep mode or screen saver. With this feature enabled in Mac OS X, the FortiGate will receive the authentication information it requires to authenticate the user and allow them access.

Note that if the user reverts their settings to disable the password requirement, this will cause the issue to reappear.

SSO using RADIUS accounting records

A FortiGate unit can authenticate users transparently who have already authenticated on an external RADIUS server. Based on the user group to which the user belongs, the security policy applies the appropriate UTM profiles. RADIUS SSO is relatively simple because the FortiGate unit does not interact with the RADIUS server, it only monitors RADIUS accounting records that the server emits. These records include the user's IP address and user group.

After the initial set-up, changes to the user database, including changes to user group memberships, are made on the external RADIUS server, not on the FortiGate unit.

This section describes:

User's view of RADIUS SSO authentication

For the user, RADIUS SSO authentication is simple:

- The user connects to the RADIUS server and authenticates.
- The user attempts to connect to a network resource that is reached through a FortiGate unit. Authentication is required for access, but the user connects to the destination without being asked for logon credentials because the FortiGate unit knows that the user is already authenticated. FortiOS applies UTM features appropriate to the user groups that the user belongs to.

Configuration Overview

The general steps to implement RADIUS Single Sign-On are:

1. If necessary, configure your RADIUS server. The user database needs to include user group information and the server needs to send accounting messages.
2. Create the FortiGate RADIUS SSO agent.
3. Define local user groups that map to RADIUS groups.
4. Create a security policy which specifies the user groups that are permitted access.

Configuring the RADIUS server

You can configure FortiGate RSSO to work with most RADIUS-based accounting systems. In most cases, you only need to do the following to your RADIUS accounting system:

- Add a user group name field to customer accounts on the RADIUS server so that the name is added to the RADIUS Start record sent by the accounting system to the FortiOS unit. User group names do not need to be added for all users, only to the accounts of users who will use RSSO feature on the FortiGate unit.
- Configure your accounting system to send RADIUS Start records to the FortiOS unit. You can send the RADIUS Start records to any FortiGate network interface. If your FortiGate unit is operating with virtual domains (VDOMs) enabled, the RADIUS Start records must be sent to a network interface in the management VDOM.

Creating the FortiGate RADIUS SSO agent

Once you define a RADIUS SSO (RSSO) agent, the FortiGate unit will accept user logon information from any RADIUS server that has the same shared secret. You can create only one RSSO agent in each VDOM.

Before you create the RSSO agent, you need to allow RADIUS accounting information on the interface that connects to the RADIUS server.

To enable RADIUS access on the interface - web-based manager:

1. Go to **System > Network > Interfaces** and edit the interface to which the RADIUS server connected.
2. Select **Listen for RADIUS Accounting Messages**.
3. Select **OK**.

To enable RADIUS access on the interface - CLI:

In this example, the port2 interface is used.

```
config system interface
   edit port2
      set allowaccess radius-acct
   end
```

To create a RADIUS SSO agent:

1. Go to **User & Device > Authentication > Single Sign-On** and select **Create New**.
2. In **Type**, select **RADIUS Single-Sign-On Agent**.
3. Select **Use RADIUS Shared Secret** and enter the RADIUS server shared secret.
4. Select **Send RADIUS Responses**.
5. Select **OK**.

To create a RADIUS SSO agent - CLI

```
config user radius
   edit RSSO_Agent
      set rsso enable
```

```
    set rsso-validate-request-secret enable
    set rsso-secret <your secret>
    set rsso-radius-response enable
end
```

Selecting which RADIUS attributes are used for RSSO

For RADIUS SSO to work, FortiOS needs to know the user's endpoint identifier (usually IP address) and RADIUS user group. There are default RADIUS attributes where FortiOS expects this information, but you can change these attributes in the `config user radius` CLI command.

RSSO information and RADIUS attribute defaults

RSSO Information	RADIUS Attribute	CLI field
Endpoint identifier	Calling-Station-ID	`rsso-endpoint-attribute`
Endpoint block attribute	Called-Station-ID	`rsso-endpoint-block-attribute`
User group	Class	`sso-attribute`

The Endpoint block attribute can be used to block or allow a user. If the attribute value is set to the name of an attribute that indicates whether to block or allow, FortiOS blocks or allows respectively all traffic from that user's IP address. The RSSO fields are visible only when `rsso` is set to `enable`.

Configuring logging for RSSO

In the `config user radius` CLI command, you can set the following flags in the `rsso-log-flags` field to determine which types of RSSO-related events are logged:

- `protocol-error` — A RADIUS protocol error occurred.
- `profile-missing` — FortiOS cannot find a user group name in a RADIUS start message that matches the name of an RSSO user group in FortiOS.
- `accounting-stop-missed` — a user context entry expired without FortiOS receiving a RADIUS Stop message.
- `accounting-event` — FortiOS did not find the expected information in a RADIUS record.
- `endpoint-block` — FortiOS blocked a user because the RADIUS record's endpoint block attribute had the value "Block".
- `radiusd-other` — Other events, described in the log message.

Defining local user groups for RADIUS SSO

You cannot use RADIUS user groups directly in security policies. Instead, you create locally-defined user groups on the FortiGate unit and associate each of them with a RADIUS user group.

To define local user groups for RADIUS SSO:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter a Name for the user group.
3. In **Type**, select **RADIUS Single Sign-On (RSSO)**.
4. In **RADIUS Attribute Value**, enter the name of the RADIUS user group this local user group represents.
5. Select **OK**.

To define local user groups for RADIUS SSO:

This example creates an RSSO user group called RSSO-1 that is associated with RADIUS user group “student”.

```
config user group
   edit RSSO-1
      set group-type rsso
      set sso-attribute-value student
   end
```

Creating security policies

RADIUS SSO uses regular identity-based security policies. The RSSO user group you specify determines which users are permitted to use the policy. You can create multiple policies if user groups can have different UTM features enabled, different permitted services, schedules, and so on.

To create a security policy for RSSO - web-based manager:

1. Go to **Policy & Objects > Policy > IPv4**.
2. Select **Create New**.
3. Enter the following information.

Incoming Interface	as needed
Source Address	as needed
Source User(s)	Select the user groups you created for RSSO. See Defining local user groups for RADIUS SSO on page 172.
Outgoing Interface	as needed
Destination Address	all
Schedule	as needed
Service	as needed
Action	ACCEPT
Enable NAT	Selected
Security Profiles	Select security profiles appropriate for the user group.

4. Select **OK**.

To ensure an RSSO-related policy is matched first, the policy should be placed higher in the security policy list than more general policies for the same interfaces.

5. Select **OK**.

To create a security policy for RSSO - CLI:

In this example, an internal network to Internet policy enables web access for members of a student group and activates the appropriate UTM profiles.

```
config firewall policy
   edit 0
      set srcintf internal
      set dstintf wan1
      set srcaddr all
      set dstaddr "all"
      set action accept
      set rsso enable
      set groups "RSSO-student"
      set schedule always
      set service HTTP HTTPS
      set nat enable
      set utm-status enable
      set av-profile students
      set webfilter-profile students
      set spamfilter-profile students
      set dlp-sensor default
      set ips-sensor default
      set application-list students
      set profile-protocol-options "default"
   end
```

Example: webfiltering for student and teacher accounts

The following example uses RADIUS SSO to apply web filtering to students, but not to teachers. Assume that the RADIUS server is already configured to send RADIUS Start and Stop records to the FortiGate unit. There are two RADIUS user groups, **students** and **teachers**, recorded in the default attribute **Class**. The workstations are connected to port1, port2 connects to the RADIUS server, and port3 connects to the Internet.

Configure the student web filter profile:

1. Go to **Security Profiles > Web Filter** and select **Create New** (the "+" button).
2. Enter the following and select **OK**.

Name	student
Inspection Mode	Proxy
FortiGuard Categories	Enable. Right-click the **Potentially Liable** category and select **Block**. Repeat for **Adult/Mature Content** and **Security Risk**.

Create the RADIUS SSO agent:

1. Go to **User & Device > Authentication > Single Sign-On** and select **Create New**.
2. In **Type**, select **RADIUS Single-Sign-On**.
3. Select **Use RADIUS Shared Secret** and enter the RADIUS server shared secret.
4. Select **Send RADIUS Responses**.
5. Select **OK**.

Define local user groups associated with the RADIUS SSO user groups:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter the following and select **OK**.

Name	RSSO-students
Type	RADIUS Single Sign-On (RSSO)
RADIUS Attribute Value	students

3. Select **Create New**, enter the following and select **OK**.

Name	RSSO-teachers
Type	RADIUS Single Sign-On (RSSO)
RADIUS Attribute Value	teachers

Create a security policy for students:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter

Incoming Interface	port1
Source Address	all
Source User(s)	RSSO-students
Source Device Type	All
Outgoing Interface	port3
Destination Address	all
Schedule	always
Service	HTTP, HTTPS
Action	ACCEPT

NAT	ON
Security Profiles	Enable AntiVirus, Web Filter, IPS. In Web Filter, select the **student** profile.

3. Select **OK**.

Create a security policy for teachers:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter

Incoming Interface	port2
Source Address	all
Source User(s)	RSSO-teachers
Source Device Type	All
Outgoing Interface	port3
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
NAT	ON
Security Profiles	Enable AntiVirus and IPS.

3. Select **OK**.

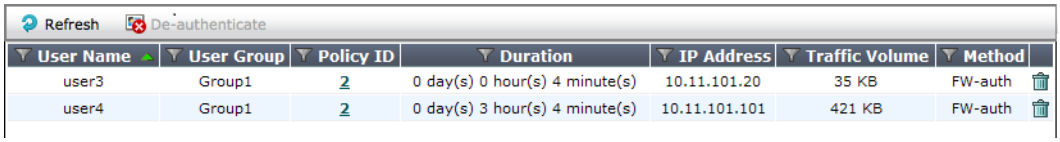
Monitoring authenticated users

This section describes how to view lists of currently logged-in firewall and VPN users. It also describes how to disconnect users.

The following topics are included in this section:

Monitoring firewall users

To monitor firewall users, go to **User & Device > Monitor > Firewall.**



You can de-authenticate a user by selecting the Delete icon for that entry.

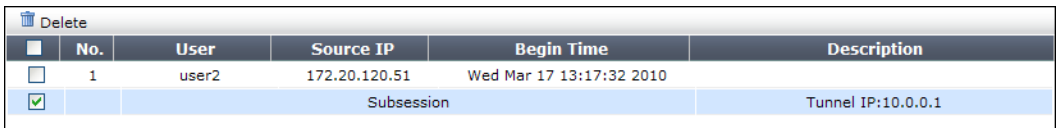
You can filter the list of displayed users by selecting the funnel icon for one of the column titles or selecting **Filter Settings**.

Optionally, you can de-authenticate multiple users by selecting them and then selecting **De-authenticate**.

Monitoring SSL VPN users

You can monitor web-mode and tunnel-mode SSL VPN users by username and IP address.

To monitor SSL VPN users, go to **VPN > Monitor > SSL-VPN Monitor**. To disconnect a user, select the user and then select the **Delete** icon.



The first line, listing the username and IP address, is present for a user with either a web-mode or tunnel-mode connection. The Subsession line is present only if the user has a tunnel mode connection. The **Description** column displays the virtual IP address assigned to the user's tunnel-mode connection.

For more information about SSL VPN, see the FortiOS Handbook SSL VPN guide.

To monitor SSL VPN users - CLI:

To list all of the SSL VPN sessions and their index numbers:

```
execute vpn sslvpn list
```

The output looks like this:

```
SSL-VPN Login Users:
 Index   User   Auth Type   Timeout         From      HTTPS in/out
 0       user1  1           256       172.20.120.51   0/0

SSL-VPN sessions:
 Index   User   Source IP        Tunnel/Dest IP
 0       user2  172.20.120.51    10.0.0.1
```

You can use the Index value in the following commands to disconnect user sessions:

To disconnect a tunnel-mode user

```
execute vpn sslvpn del-tunnel <index>
```

To disconnect a web-mode user

```
execute vpn sslvpn del-web <index>
```

You can also disconnect multiple users:

To disconnect all tunnel-mode SSL VPN users in this VDOM

```
execute vpn ssl del-all tunnel
```

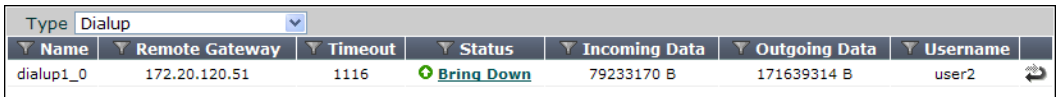
To disconnect all SSL VPN users in this VDOM

```
execute vpn ssl del-all
```

Monitoring IPsec VPN users

To monitor IPsec VPN tunnels in the web-based manager, go to **VPN > Monitor > IPsec Monitor**. user names are available only for users who authenticate with XAuth.

You can close a tunnel by selecting the tunnel and right click to select **Bring Down**.



For more information, see the FortiOS Handbook IPsec VPN guide.

Monitoring users Quarantine

The User Quarantine list shows all IP addresses and interfaces blocked by NAC quarantine. The list also shows all IP addresses, authenticated users, senders, and interfaces blocked by Data Leak Prevention (DLP). The system administrator can selectively release users or interfaces from quarantine or configure quarantine to expire after a selected time period.

All sessions started by users or IP addresses on the User Quarantine list are blocked until the user or IP address is removed from the list. All sessions to an interface on the list are blocked until the interface is removed from the list.

You can configure NAC quarantine to add users or IP addresses to the User Quarantine list under the following conditions:

- **Users or IP addresses that originate attacks detected by IPS** - To quarantine users or IP addresses that originate attacks, enable and configure **Quarantine** in an IPS Filter.
- **Users or IP addresses that are quarantined by Data Leak Prevention** - In a DLP sensor select **Quarantine IP Address** as the action to take.

For more information, see FortiOS Handbook Security Profiles guide.

Users are viewed from **User & Device > Monitor > User Quarantine.**

Delete	Removes the selected user or IP address from the User Quarantine list.
Remove All	Removes all users and IP addresses from the User Quarantine list.
Search	Search the list for a particular IP address.
Source	The FortiGate function that caused the user or IP address to be added to the User Quarantine list: IPS or Data Leak Prevention.
Created	The date and time the user or IP address was added to the Banned User list.
Expires	The date and time the user or IP address will be automatically removed from the User Quarantine list. If **Expires** is **Indefinite**, you must manually remove the user or host from the list.

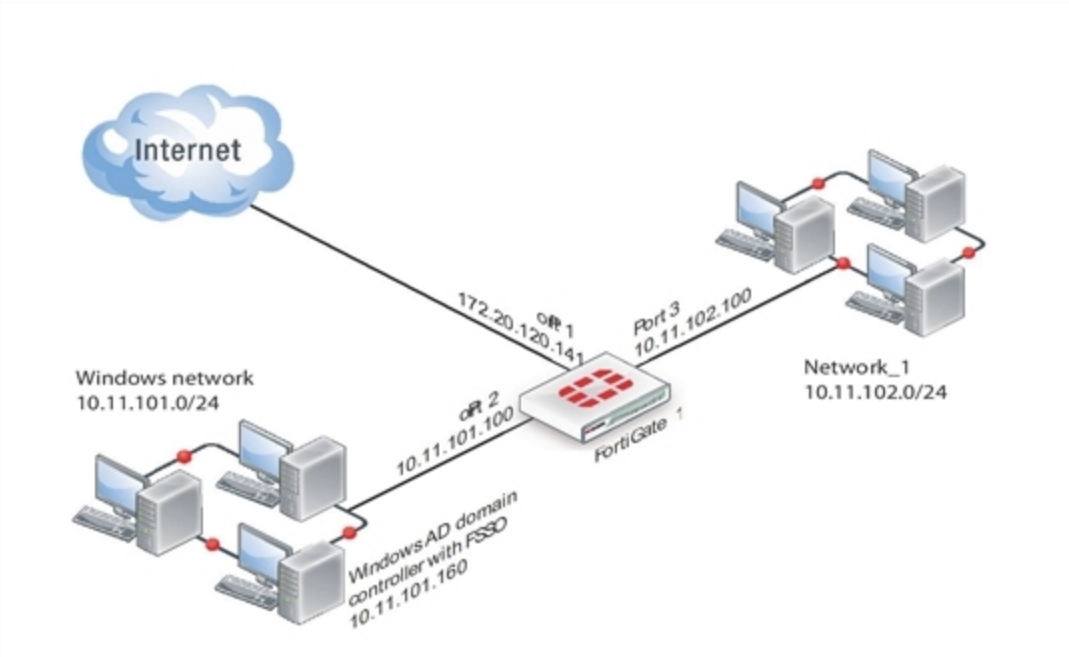
Examples and Troubleshooting

This chapter provides an example of a FortiGate unit providing authenticated access to the Internet for both Windows network users and local users.

The following topics are included in this section:

Firewall authentication example

Example configuration



Overview

In this example, there is a Windows network connected to Port 2 on the FortiGate unit and another LAN, Network_1, connected to Port 3.

All Windows network users authenticate when they logon to their network. Members of the Engineering and Sales groups can access the Internet without entering their authentication credentials again. The example assumes that the Fortinet Single Sign On (FSSO) has already been installed and configured on the domain controller.

LAN users who belong to the Internet_users group can access the Internet after entering their username and password to authenticate. This example shows only two users, User1 is authenticated by a password stored on the FortiGate unit, User2 is authenticated on an external authentication server. Both of these users are referred to as local users because the user account is created on the FortiGate unit.

Creating a locally-authenticated user account

User1 is authenticated by a password stored on the FortiGate unit. It is very simple to create this type of account.

To create a local user - web-based manager:

1. Go to **User & Device > User > User Definition** and select **Create New**.
2. Follow the User Creation Wizard, entering the following information and then select **Create**:

User Type	Local User
User Name	User1
Password	hardtoguess
Email Address **SMS**	(optional)
Enable	Select.

To create a local user - CLI:

```
config user local
   edit user1
      set type password
      set passwd hardtoguess
   end
```

Creating a RADIUS-authenticated user account

To authenticate users using an external authentication server, you must first configure the FortiGate unit to access the server.

To configure the remote authentication server - web-based manager:

1. Go to **User & Device > Authentication > RADIUS Servers** and select **Create New**.
2. Enter the following information and select **OK**:

Name	OurRADIUSsrv
Primary Server Name/IP	10.11.101.15
Primary Server Secret	OurSecret
Authentication Scheme	Select **Use Default Authentication Scheme**.

To configure the remote authentication server - CLI:

```
config user radius
   edit OurRADIUSsrv
      set server 10.11.102.15
      set secret OurSecret
      set auth-type auto
   end
```

Creation of the user account is similar to the locally-authenticated account, except that you specify the RADIUS authentication server instead of the user's password.

To configure a remote user - web-based manager:

1. Go to **User & Device > User > User Definition** and select **Create New**.
2. Follow the User Creation Wizard, entering the following information and then select **Create**:

User Type	Remote RADIUS User
User Name	User2
RADIUS server	OurRADIUSsrv
Email Address **SMS**	(optional)
Enable	Select

To configure a remote user - CLI:

```
config user local
   edit User2
      set name User2
      set type radius
      set radius-server OurRADIUSsrv
   end
```

Creating user groups

There are two user groups: an FSSO user group for FSSO users and a firewall user group for other users. It is not possible to combine these two types of users in the same user group.

Creating the FSSO user group

For this example, assume that FSSO has already been set up on the Windows network and that it uses Advanced mode, meaning that it uses LDAP to access user group information. You need to

- configure LDAP access to the Windows AD global catalog
- specify the collector agent that sends user logon information to the FortiGate unit
- select Windows user groups to monitor
- select and add the Engineering and Sales groups to an FSSO user group

To configure LDAP for FSSO - web-based manager:

1. Go to **User & Device > Authentication > LDAP Servers** and select **Create New**.
2. Enter the following information:

Name	ADserver
Server Name / IP	10.11.101.160
Distinguished Name	dc=office,dc=example,dc=com
Bind Type	Regular
User DN	cn=FSSO_Admin,cn=users,dc=office,dc=example,dc=com
Password	set_a_secure_password

3. Leave other fields at their default values.
4. Select **OK**.

To configure LDAP for FSSO - CLI"

```
config user ldap
   edit "ADserver"
      set server "10.11.101.160"
      set dn "cn=users,dc=office,dc=example,dc=com"
      set type regular
      set username "cn=administrator,cn=users,dc=office,dc=example,dc=com"
      set password set_a_secure_password
   next
end
```

To specify the collector agent for FSSO - web-based manager

1. Go to **User & Device > Authentication > Single Sign-On** and select **Create New.**
2. Enter the following information:

Type	Fortinet Single Sign-On Agent
Name	WinGroups
Primary Agent IP/Name	10.11.101.160
Password	fortinet_canada
LDAP Server	ADserver

3. Select **Apply & Refresh**.

In a few minutes, the FortiGate unit downloads the list of user groups from the server.

To specify the collector agent for FSSO - CLI:

```
config user fsso
```

```
edit "WinGroups"
   set ldap-server "ADserver"
   set password ENC
       G7GQV7NEqilCM9jKmVmJJFVvhQ2+wtNEe9T0iYA5Sa+EqT2J8zhOrbkJFDr0RmY3c4LaoXdsoBczA
       1dONmcGfthTxxwGsigzGpbJdC71spFlQYtj
   set server "10.11.101.160"
end
```

To create the FSSO_Internet-users user group - web-based manager:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter the following information and then select **OK**:

Name	FSSO_Internet_users
Type	Fortinet Single Sign-On (FSSO)
Members	Engineering, Sales

To create the FSSO_Internet-users user group - CLI:

```
config user group
   edit FSSO_Internet_users
      set group-type fsso-service
      set member CN=Engineering,cn=users,dc=office,dc=example,dc=com
          CN=Sales,cn=users,dc=office,dc=example,dc=com
   end
```

Creating the Firewall user group

The non-FSSO users need a user group too. In this example, only two users are shown, but additional members can be added easily.

To create the firewall user group - web-based manager:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter the following information and then select **OK**:

Name	Internet_users
Type	Firewall
Members	User1, User2

To create the firewall user group - CLI:

```
config user group
   edit Internet_users
      set group-type firewall
      set member User1 User2
   end
```

Defining policy addresses

1. Go to **Policy & Objects > Objects > Addresses**.
2. Create the following addresses:

Address Name	Internal_net
Type	Subnet
Subnet / IP Range	10.11.102.0/24
Interface	Port 3

Address Name	Windows_net
Type	Subnet
Subnet / IP Range	10.11.101.0/24
Interface	Port 2

Creating security policies

Two security policies are needed: one for firewall group who connect through port3 and one for FSSO group who connect through port2.

To create a security policy for FSSO authentication - web-based manager:

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information:

Incoming Interface	Port2
Source Address	Windows_net
Source User(s)	FSSO_Internet_users
Outgoing Interface	Port1
Destination Address	all
Schedule	always
Service	ALL
NAT	ON
Security Profiles	Optionally, enable security profiles.

3. Select OK.

To create a security policy for FSSO authentication - CLI:

```
config firewall policy
   edit 0
      set srcintf port2
      set dstintf port1
      set srcaddr Windows_net
      set dstaddr all
      set action accept
      set groups FSSO_Internet_users
      set schedule always
      set service ANY
      set nat enable
   end
```

To create a security policy for local user authentication - web-based manager

1. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.
2. Enter the following information:

Incoming Interface	Port3
Source Address	Internal_net
Source User(s)	Internet_users
Outgoing Interface	Port1
Destination Address	all
Schedule	always
Service	ALL
NAT	ON
Security Profiles	Optionally, enable security profiles.

3. Select **OK**.

To create a security policy for local user authentication - CLI

```
config firewall policy
   edit 0
      set srcintf port3
      set dstintf port1
      set srcaddr internal_net
      set dstaddr all
      set action accept
      set schedule always
      set groups Internet_users
      set service ANY
      set nat enable
   end
```

LDAP Dial-in using member-attribute example

In this example, users defined in MicroSoft Windows Active Directory (AD) are allowed to set up a VPN connection simply based on an attribute that is set to TRUE, instead of based on their user group. In AD the "Allow Dialin" property is activated in the user properties, and this sets the `msNPAllowDialin` attribute to "TRUE".

This same procedure can be used for other member attributes, as your system requires.

To accomplish this with a FortiGate unit, member-attribute must be set. This can only be accomplished through the CLI - the option is not available through the web-based manager.

Before configuring the FortiGate unit, ensure the AD server has the `msNPAllowDialin` attribute set to "TRUE" for the users in question. If not, those users will not be able to authenticate.

To configure user LDAP member-attribute settings - CLI:

```
config user ldap
   edit "ldap_server"
      set server "192.168.201.3"
      set cnid "sAMAccountName"
      set dn "DC=fortilabanz,DC=com,DC=au"
      set type regular
      set username "fortigate@sample.com"
      set password ******
      set member-attr "msNPAllowDialin"
   next
end
```

To configure LDAP group settings - CLI:

```
config user group
   edit "ldap_grp"
      set member "ldap"
      config match
         edit 1
            set server-name "ldap"
            set group-name "TRUE"
         next
      end
   next
end
```

Once these settings are in place, users that are a member of the `ldap` user group will be able to authenticate.

To ensure your settings are correct, here is the sample output from a diag debug command that shows the authentication process.

When the "Allow Dial-in" attribute is set to "TRUE" the following will likely be in the output:

```
get_member_of_groups-Get the memberOf groups.
get_member_of_groups- attr='msNPAllowDialin', found 1 values
get_member_of_groups-val[0]='TRUE'
fnbamd_ldap_get_result-Auth accepted
```

```
fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth_poll_ldap-Result for ldap svr 192.168.201.3 is SUCCESS
fnbamd_auth_poll_ldap-Passed group matching
```

If the attribute is not set but it is expected, the following will likely be in the output:

```
get_member_of_groups-Get the memberOf groups.
get_member_of_groups- attr='msNPAllowDialin', found 1 values
get_member_of_groups-val[0]='FALSE'
fnbamd_ldap_get_result-Auth accepted
fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth_poll_ldap-Result for ldap svr 192.168.201.3 is SUCCESS
fnbamd_auth_poll_ldap-Failed group matching
```

The only difference between these two outputs is the last line which is either passed or failed based on if the member-attribute is set to the expected value or not.

RADIUS SSO example

A common RADIUS SSO topology involves a medium sized company network of users connecting to the Internet through the FortiGate unit, and authenticating with a RADIUS server. RADIUS SSO authentication was selected because it is fast and relatively easy to configure.

This section includes:

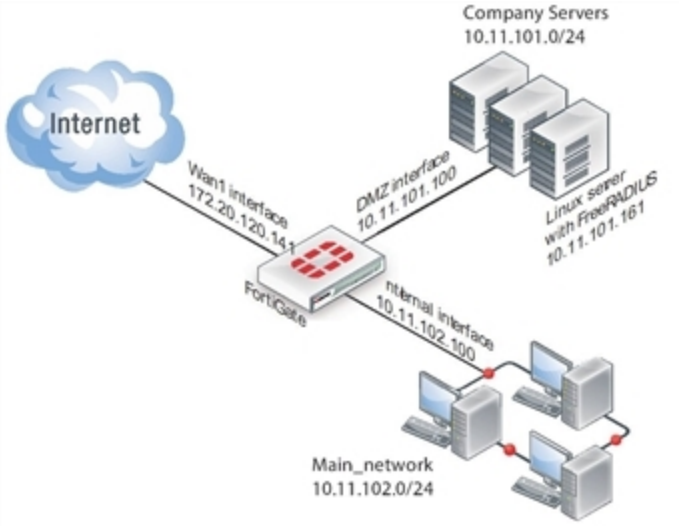
Assumptions

- VDOMs are not enabled
- The admin super_admin administrator account will be used for all FortiGate unit configuration.
- Any other devices on the network do not affect the topology of this example, and therefore are not included.
- Anywhere settings are not described, they are assumed to be default values.
- A RADIUS server is installed on a server or FortiAuthenticator unit and uses default attributes.
- BGP is used for any dynamic routing.
- Authentication event logging under Log&Report has been configured.

Topology

Example.com has an office with 20 users on the internal network. These users need access to the Internet to do their jobs. The office network is protected by a FortiGate-60C unit with access to the Internet through the wan1 interface, the user network on the internal interface, and all the servers are on the DMZ interface. This includes an Ubuntu Linux server running FreeRADIUS. For this example only two users will be configured — Pat Lee with an account name `plee`, or `plee@example.com`, and Kelly Green with an account name `kgreen`, or `kgreen@example.com`.

RADIUS SSO topology



Configuring RADIUS

Configuring RADIUS includes configuring the RADIUS server such as FreeRADIUS, a radius client on user's computers, and configuring users in the system. For this example the two users will be Pat Lee, and Kelly Green. They belong to a group called `exampledotcom_employees`. When it is all configured, the RADIUS daemon needs to started.

The users have a RADIUS client installed on their PCs that allows them to authenticate through the RADIUS server.

FreeRADIUS can be found on the freeradius.org website. For any problems installing FreeRADIUS, see the FreeRADIUS documentation.

Configuring FortiGate interfaces

Before configuring the RADIUS SSO security policy, configure FortiGate interfaces. This includes defining a DHCP server for the internal network as this type of network typically uses DHCP. The wan1 and dmz interfaces are assigned static IP addresses and do not need a DHCP server.

FortiGate interfaces used in this example

Interface	Subnet	Act as DHCP Server	Devices
wan1	172.20.120.141	No	Internet Service Provider
dmz	10.11.101.100	No	Servers, including RADIUS server
internal	10.11.102.100	Yes: x.x.x.110-.250	Internal user network

To configure FortiGate interfaces - web-based manager:

1. Go to **System > Network > Interfaces**.
2. Select wan1 to edit.
3. Enter the following information and select **OK**.

Alias	Internet
Addressing Mode	Manual
IP/Network Mask	172.20.120.141/255.255.255.0
Administrative Access	HTTPS, SSH
Enable DHCP Server	Not selected
Comments	Internet
Administrative Status	Up

4. Select dmz to edit.
5. Enter the following information and select **OK**.

Alias	Servers
Addressing Mode	Manual
IP/Network Mask	10.11.101.100/255.255.255.0
Administrative Access	HTTPS, SSH, PING, SNMP
Enable DHCP Server	Not selected
Listen for RADIUS Accounting Messages	Select
Comments	Servers
Administrative Status	Up

6. Select internal to edit.
7. Enter the following information and select **OK**.

Alias	Internal network
Addressing Mode	Manual
IP/Network Mask	10.11.102.100/255.255.255.0
Administrative Access	HTTPS, SSH, PING

Enable DHCP Server	Select
Address Range	10.11.102.110 - 10.11.102.250
Netmask	255.255.255.0
Default Gateway	Same as Interface IP
DNS Server	Same as System DNS
Comments	Internal network
Administrative Status	Up

Configuring a RADIUS SSO Agent on the FortiGate unit

To create a RADIUS SSO agent:

1. Go to **User & Device > Authentication > Single Sign-On** and select **Create New**.
2. In **Type**, select **RADIUS Single-Sign-On Agent**.
3. Select **Use RADIUS Shared Secret** and enter the RADIUS server shared secret.
4. Select **Send RADIUS Responses**.
5. Select **OK**.
   The Single Sign-On agent is named RSSO_Agent.

Creating a RADIUS SSO user group

To define a local user group for RADIUS SSO:

1. Go to **User & Device > User > User Groups** and select **Create New**.
2. Enter a Name for the user group.
3. In **Type**, select **RADIUS Single Sign-On (RSSO)**.
4. In **RADIUS Attribute Value**, enter the name of the RADIUS user group this local user group represents.
5. Select **OK**.

Configuring FortiGate regular and RADIUS SSO security policies

With the RADIUS server and FortiGate interfaces configured, security policies can be configured. This includes both RADIUS SSO and regular policies, as well as addresses and address groups. All policies require NAT to be enabled.

Security policies required for RADIUS SSO

Seq. No.	From -> To	Type	Schedule	Description
1	internal -> wan1	RADIUS SSO	business hours	Authenticate outgoing user traffic.

Seq. No.	From -> To	Type	Schedule	Description
2	internal -> wan1	regular	always	Allow essential network services and VoIP.
3	dmz -> wan1	regular	always	Allow servers to access Internet.
4	internal -> dmz	regular	always	Allow users to access servers.
5	any -> any	deny	always	Implicit policy denying all traffic that hasn't been matched.

The RADIUS SSO policy must be placed at the top of the policy list so it is matched first. The only exception to this is if you have a policy to deny access to a list of banned users. In this case, that policy must go at the top so the RADIUS SSO does not mistakenly match a banned user or IP address.

This section includes:

- Schedules, address groups, and services groups
- Configuring regular security policies
- Configuring RADIUS SSO security policy

Schedules, address groups, and services groups

This section lists the lists that need to be configured before security policies are created. Creating these lists is straight forward, so the essential information has been provided here but not step by step instructions. For more information on firewall related details, see

Schedules

Only one schedule needs to be configured — `business_hours`. This is a fairly standard Monday to Friday 8am to 5pm schedule, or whatever days and hours covers standard work hours at the company.

Address groups

The following address groups need to be configured before the security policies.

Address Group Name	Interface	Address range included
internal_network	internal	10.11.102.110 to 10.11.102.250
company_servers	dmz	10.11.101.110 to 10.11.101.250

Service groups

The following service groups need to be configured before the security policies. Note that the services listed are suggestions and may include more or less as required.

Service Group Name	Interface	Description of services to be included
essential_network_services	internal	Any network protocols required for normal network operation such as DNS, NTP, BGP.
essential_server_services	dmz	All the protocols required by the company servers such as BGP, HTTP, HTTPS, FTP, IMAP, POP3, SMTP, IKE, SQL, MYSQL, NTP, TRACEROUTE, SOCKs, and SNMP.
user_services	internal	Any protocols required by users HTTP, HTTP, FTP,

The following security policy configurations are basic and only include logging, and default AV and IPS.

Configuring regular security policies

Regular security policies allow or deny access for non-RADIUS SSO traffic. This is essential as there are network services—such as DNS, NTP, and FortiGuard—that require access to the Internet.

To configure regular security policies - web-based manager:

1. Go to **Policy & Objects > Policy > IP4**, and select **Create New**.
2. Enter the following information, and select **OK**.

Incoming Interface	Internal
Source Address	internal_network
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	essential_network_services
Action	ACCEPT
NAT	ON
Security Profiles	ON: AntiVirus, IPS
Log Allowed Traffic	ON
Comments	Essential network services

3. Select **Create New**, enter the following information, and select **OK**.

Incoming Interface	dmz

Source Address	company_servers
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	essential_server_services
Action	ACCEPT
NAT	ON
Security Profiles	ON: AntiVirus, IPS
Log Allowed Traffic	enable
Comments	Company servers accessing the Internet

4. Select **Create New**, enter the following information, and select **OK**.

Incoming Interface	Internal
Source Address	internal_network
Outgoing Interface	dmz
Destination Address	company_servers
Schedule	always
Service	all
Action	ACCEPT
NAT	ON
Security Profiles	ON: AntiVirus, IPS
Log Allowed Traffic	enable
Comments	Access company servers

Configuring RADIUS SSO security policy

The RADIUS SSO policy allows access for members of specific RADIUS groups.

To configure RADIUS SSO security policy:

1. Go to **Policy & Objects > Policy > IP4**.
2. Select **Create New**.
3. Enter the following information:

Incoming Interface	Internal
Source Address	internal_network
Source User(s)	Select the user groups you created for RSSO.
Outgoing Interface	wan1
Destination Address	all
Schedule	business_hours
Service	ALL
Action	ACCEPT
NAT	ON
Security Profiles	ON: AntiVirus, WebFilter, IPS, and Email Filter. In each case, select the default profile.

4. Select **OK**.
5. To ensure an RSSO-related policy is matched first, the policy should be placed higher in the security policy list than more general policies for the same interfaces.
6. Select **OK**.

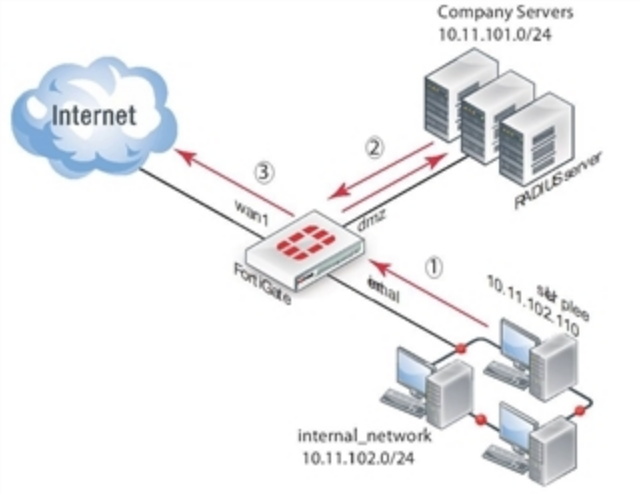
Testing

Once configured, a user only needs to log on to their PC using their RADIUS account. After that when they attempt to access an Internet website, the FortiGate unit will use their session information to get their RADIUS information. Once the user is verified, they are allowed access to the website.

To test the configuration perform the following steps:

1. Have user 'plee' logon to their PC, and try to access an Internet website.
2. The FortiGate unit will contact the RADUS server for user plee's information.
   Once confirmed, plee will have access to the website.
   Each step generates log entries that enable you to verify that each step was successful.
3. If a step is unsuccessful, confirm that your configuration is correct.

RADIUS SSO test



Troubleshooting

In the web-based manager, a good tool for troubleshooting is the packet counter column on the security policy page (**Policy > Policy**). This column displays the number of packets that have passed through this security policy. Its value when you are troubleshooting is that when you are testing your configuration (end to end connectivity, user authentication, policy use) watching the packet count for an increase confirms any other methods you may be using for troubleshooting. It provides the key of which policy is allowing the traffic, useful information if you expect a user to require authentication and it never happens. For more information about authentication security policies, see "Authentication in security policies".

This section addresses how to get more information from the CLI about users and user authentication attempts to help troubleshoot failed authentication attempts.

```
diag firewall iprope list
```
Shows the IP that the computer connected from. This is useful to confirm authorization and VPN settings.

```
diag firewall iprope clear
```
Clear all authorized users from the current list. Useful to force users to re-authenticate after system or group changes. However, this command may easily result in many users having to re-authenticate, so use carefully.

```
diag rsso query ip
diag rsso query rsso-key
```
Queries the RSSO database.

For more information on troubleshooting specific features, go to that section of this document. Most sections have troubleshooting information at the end of the section. In addition to that information, see the FortiOS Handbook Troubleshooting guide for general troubleshooting information.

Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.